
TOMORROW starts here.
cisco
Cisco live!

SDN Security

BRKSEC-2760

Alok Mittal

Security Business Group, Cisco

Cisco live!

Security at the Speed of the Network

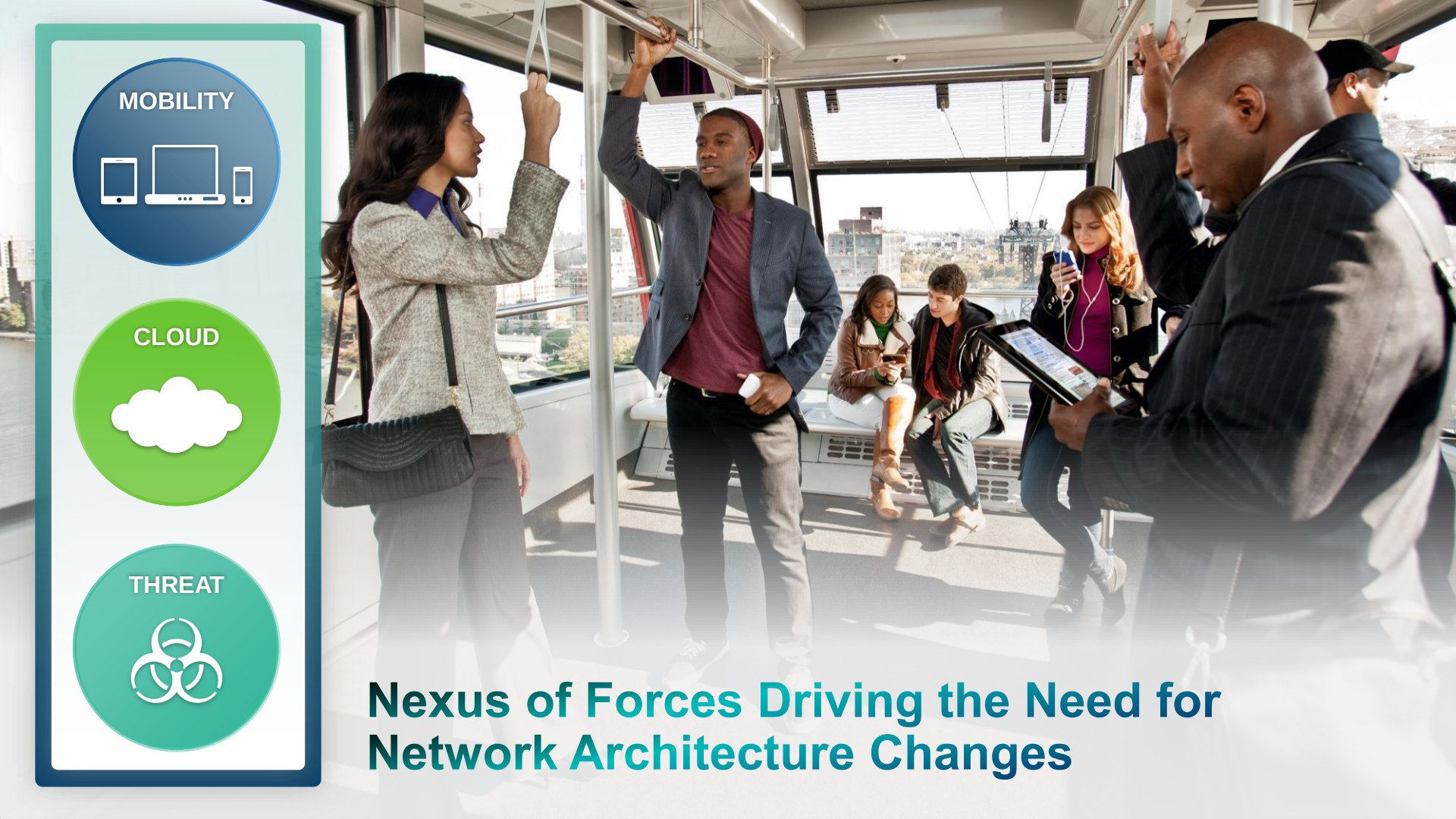
Automating and Accelerating Security Through SDN

Countering threats is complex and difficult. Software Defined Networking (SDN) offers a way to respond to attacks with the speed of the network: tying together the visibility provided by the network, and the control provided by SDN, with intelligent automation. This breakout session is targeting Network and Security professionals looking for how SDN can improve their network security architecture.

Agenda

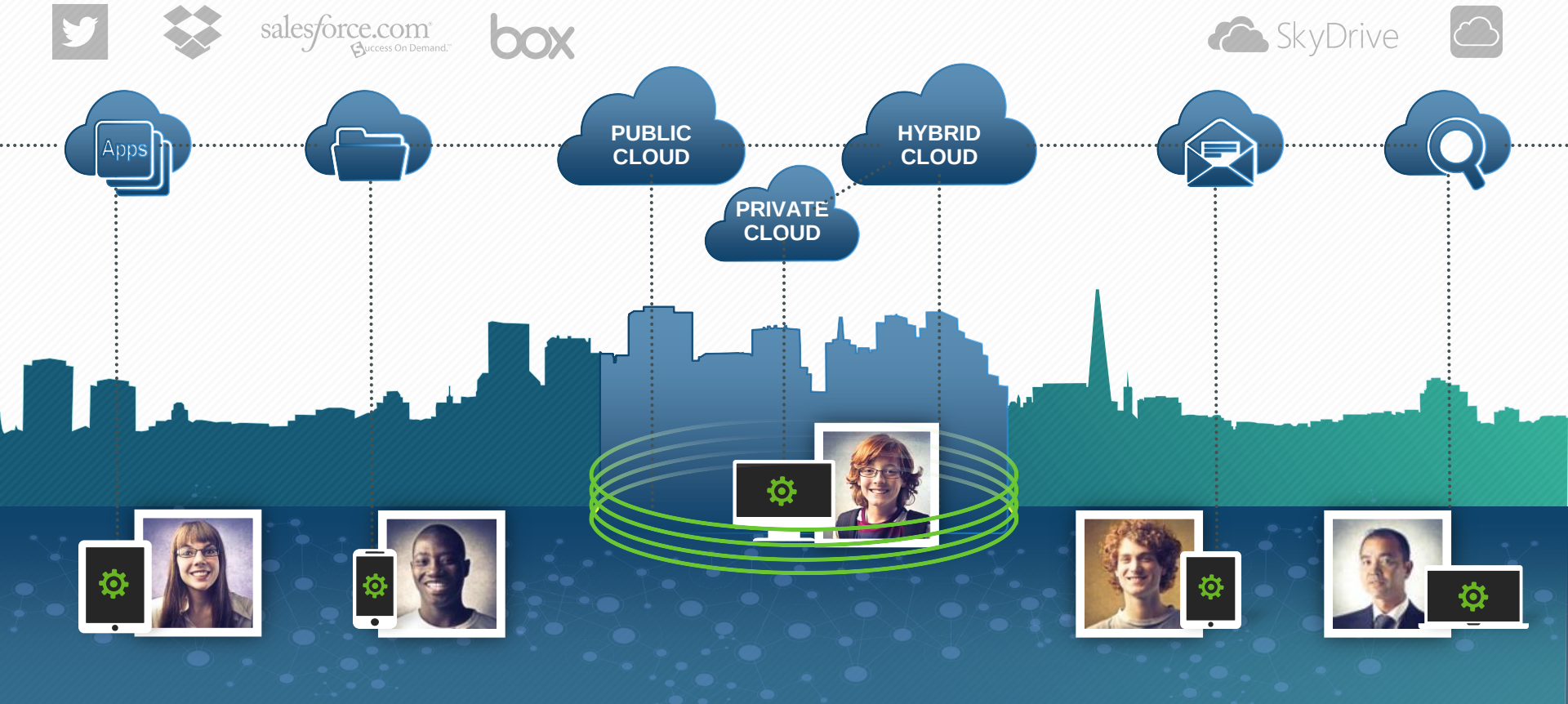
- Introduction to Current Security Challenges
- Introduction to Software Defined Networking
- Bringing the two together – How SDN can help in solving security challenges
- SDN Security Components
- Securing SDN

Introduction to Security Challenges

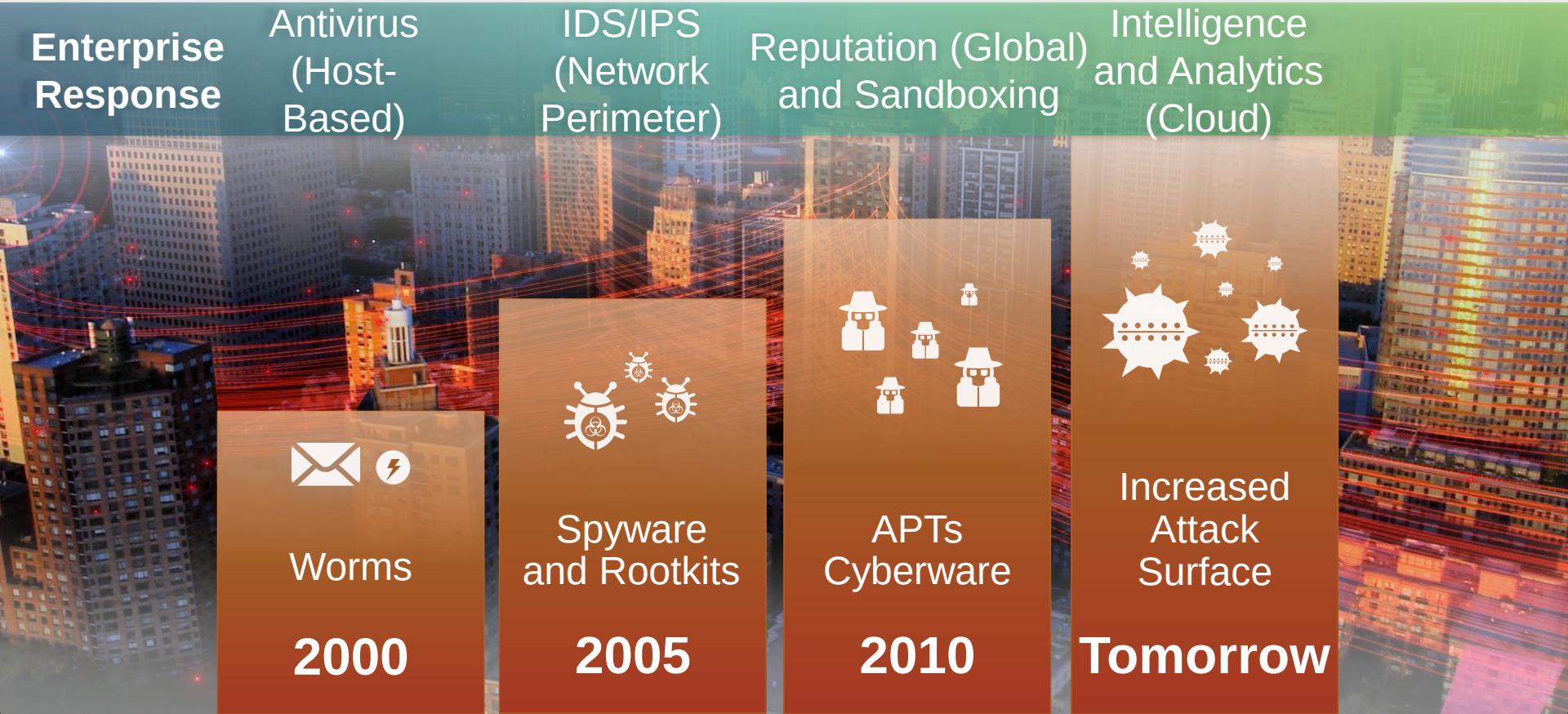


Nexus of Forces Driving the Need for Network Architecture Changes

Any Device **to Any Cloud**



The Threat Landscape is Evolving



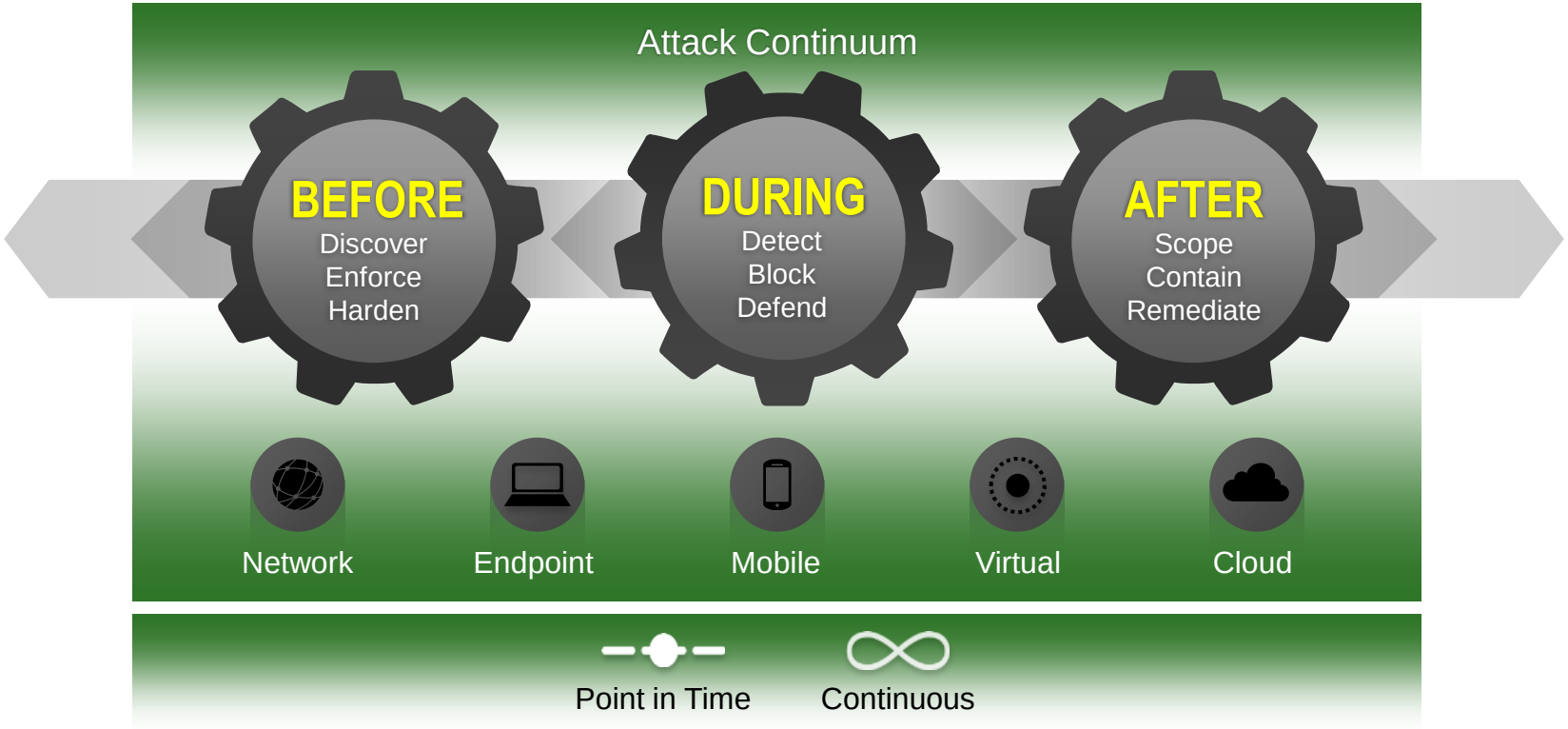
The Security Problem

Changing
Business Models

Dynamic
Threat Landscape

Complexity
and Fragmentation

The New Security Model



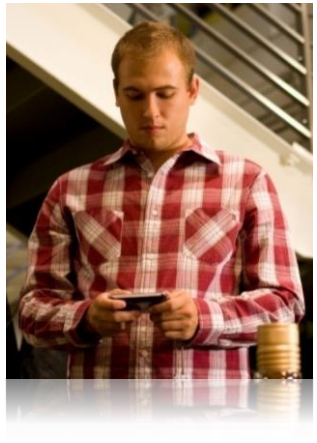
- Policy
- Access Control

- Netflow, Log, and DNS Monitoring
- Content Inspection
- Threat Analytics
- Behaviour Anomaly Detection

- Contain
- Fix

Manual Security Processes

AFTER

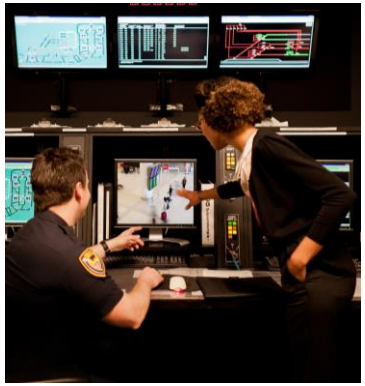


DURING

```
Internet:
Destination        Gateway            Flags        Refs      Use   Netif Expire
default            rtp-mcgrew-891.cis UGSc           19        0     en0
10.117.10.224/28   link#4             UCS             1        0     en0
rtp-mcgrew-891.cis 28:94:f:e8:b7:2c   UHLWIir        20       24     en0   1103
rtp-mcgrew-8912.ci localhost          UHS             0        0     lo0
127                localhost          UCS             0        0     lo0
localhost          localhost          UH              2      550     lo0
169.254            link#4             UCS             0        0     en0

Internet6:
Destination        Gateway            Flags        Netif Expire
localhost          link#1             UHL             lo0
fe80::%lo0         localhost          UcI             lo0
localhost          link#1             UHLI            lo0
fe80::%en0         link#4             UCI             en0
darkstar-2.local   20:cf:e9:18:ef:6d  UHLI            lo0
fe80::8a53:95ff:fe 88:53:95:7b:7b:94  UHLWIi          en0
ff01::%lo0         localhost          UmCI            lo0
ff01::%en0         link#4             UmCI            en0
ff02::%lo0         localhost          UmCI            lo0
ff02::%en0         link#4             UmCI            en0
darkstar-2:~ mcgrew$
```

BEFORE



SDN Automation: the Speed of the Network

Brief Introduction to SDN

Introduction to Software Defined Networking (SDN)?

Many Definitions

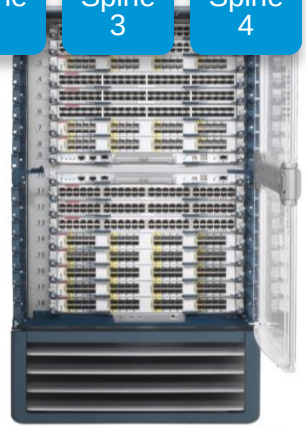
- Openflow
- Controller
- Openstack
- Overlays
- Network virtualisation
- Automation
- APIs
- Application oriented
- Virtual Services
- Open vSwitch
- …

Software Defined Networking (SDN)

Controller

Spine Nodes

Spine 1 | Spine 2 | Spine 3 | Spine 4 | Spine 5



- Supervisor - Control
- Fabric Cards - Forwarding
- Line Cards - Services

Leaf 1 | Leaf 2 | Leaf 3 | Leaf 4 | Leaf 5 | Leaf 6 | Leaf 7 | Leaf 8 | Leaf 9 | Leaf 10 | Leaf 11 | Leaf 12 | Leaf 13 | Leaf 14 | Leaf 15 | Leaf 16

Leaf Nodes

Basic Definitions

What Is Software Defined Network (SDN)?

"…In the SDN architecture, the **control and data planes are decoupled,** network intelligence and state are logically centralised, and the underlying network infrastructure is abstracted from the applications…"

Note: SDN is not mandatory for network programmability nor automation

Source: www.opennetworking.org

What Is OpenFlow?

Open protocol that specifies **interactions between de-coupled control and data planes**

Note: OF is not mandatory for SDN

Note: North-bound Controller APIs are vendor-specific

What is OpenStack?

Opensource software for building public and private Clouds; includes Compute (Nova), Networking (Quantum) and Storage (Swift) services.

Note: Applicable to SDN and non-SDN networks

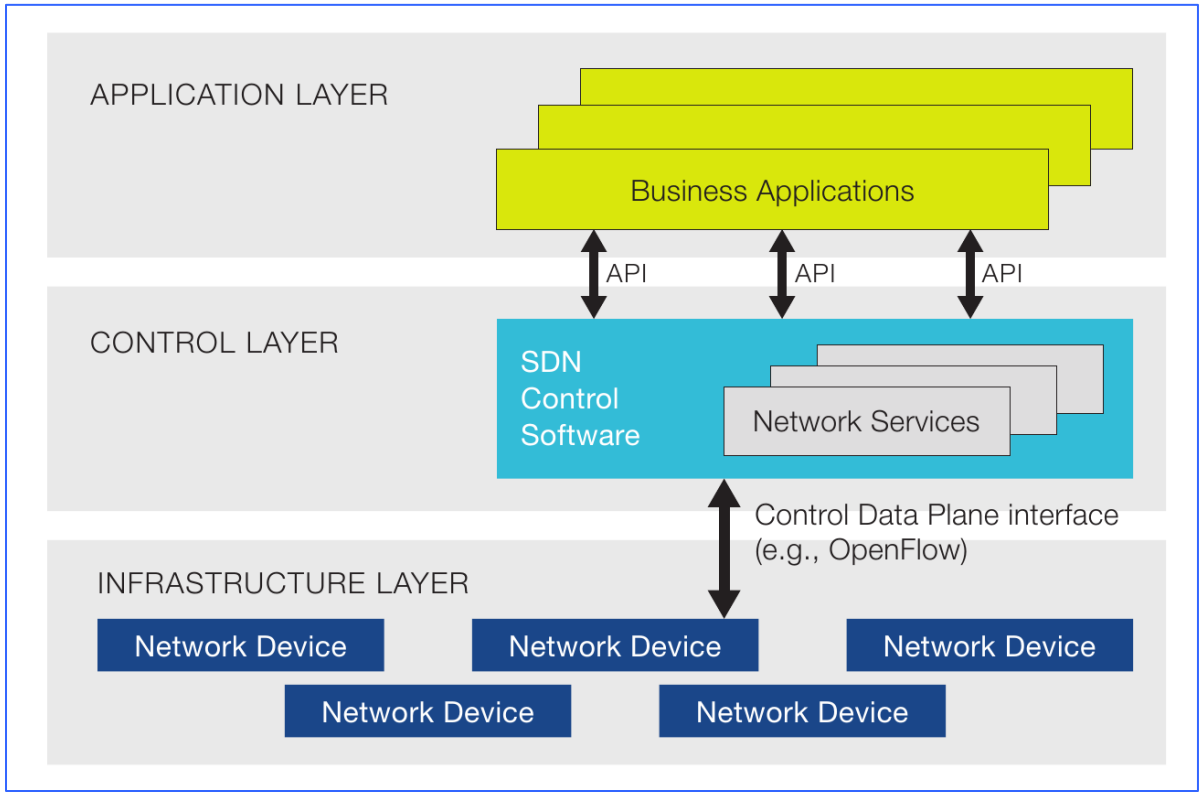
Source: www.openstack.org

What is Overlay Network?

Overlay network is created on existing network infrastructure (physical and/or virtual) using a network protocol. Examples of overlay network protocol are: GRE, VPLS, OTV, LISP and VXLAN

Note: Applicable to SDN and non-SDN networks

Basic Architecture in all Models



Key SDN Goals and Concepts

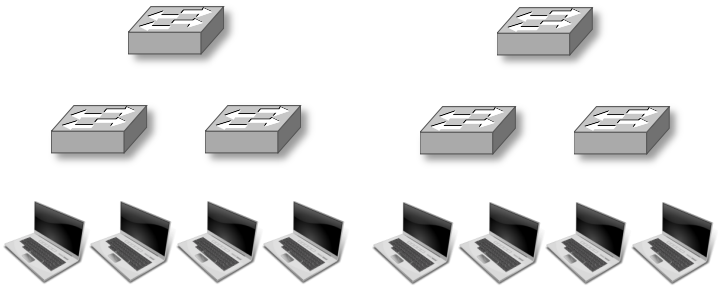
- There is a controller than centralises network configuration and attempts to makes networks easier to provision and configure
- Network intelligence and state are logically centralised, and the underlying network infrastructure is abstracted from the applications
- Enables automation - to better able to respond to the changing needs of business applications and users
- Examples -
  - Network topology changes can be made without manually reconfiguring network devices
  - Based on application requirements, virtual networks can be created
  - Security controls do not have to physically exist at a particular network location

Network Programmability

Network Monitoring

Bandwidth Management

Load Balancing

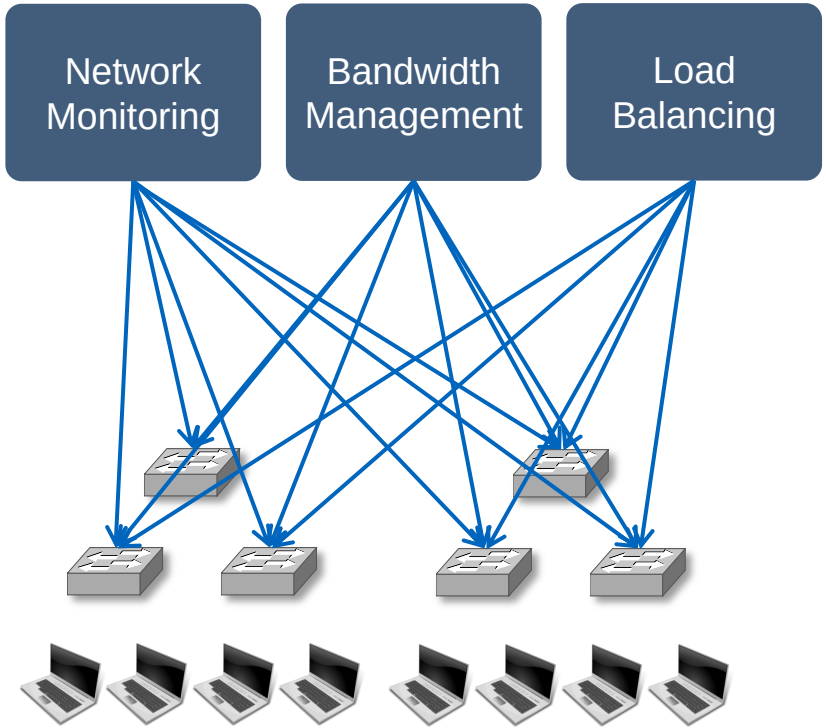


Network Programmability

SNMP

CLI

NetFlow

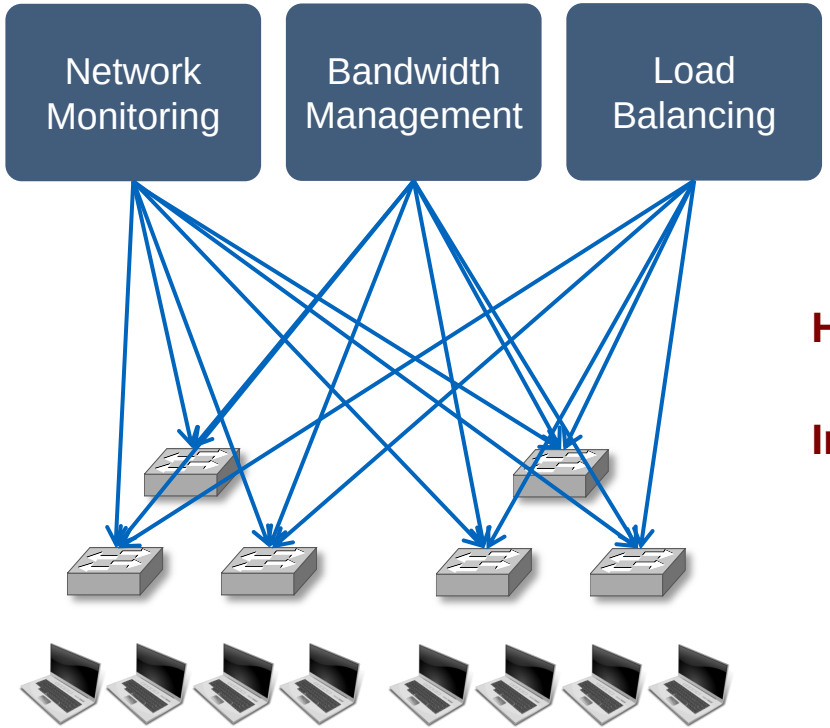


Network Programmability

SNMP

CLI

NetFlow



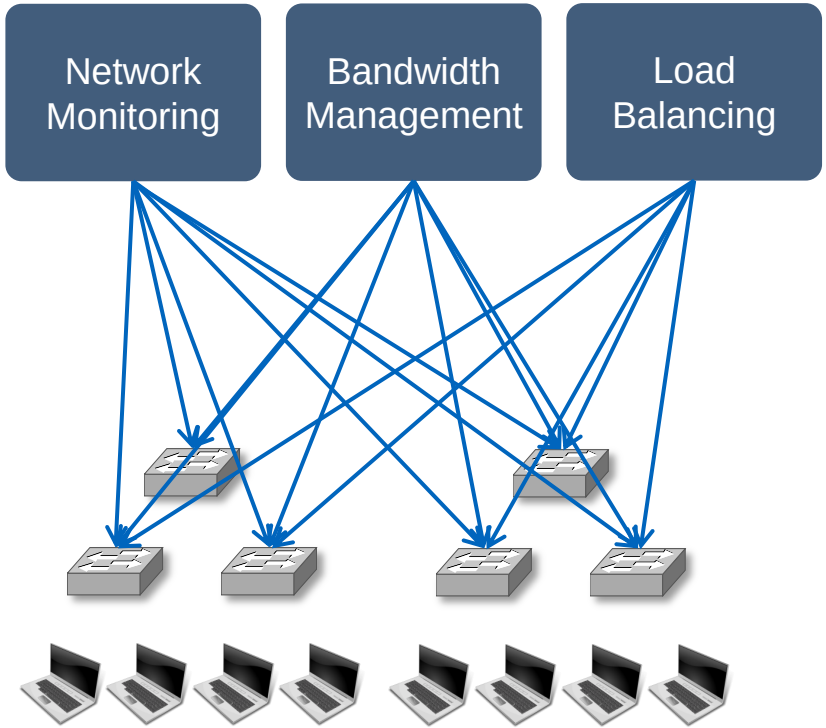
Heterogeneous devices

Inconsistent data models

Network Programmability

Programmatic Interfaces

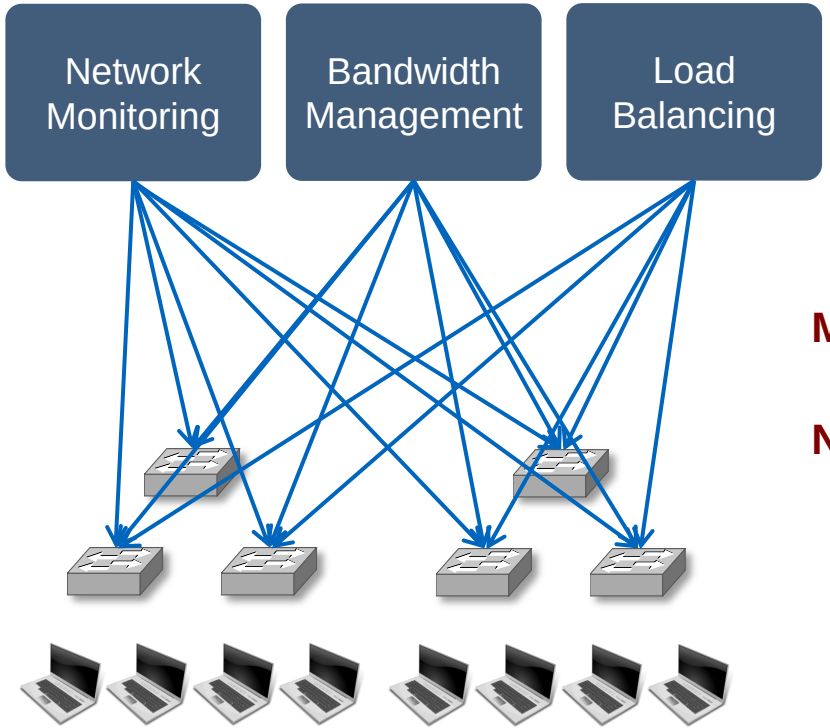
onePK



Network Programmability

Programmatic Interfaces

onePK



Multiple topology models

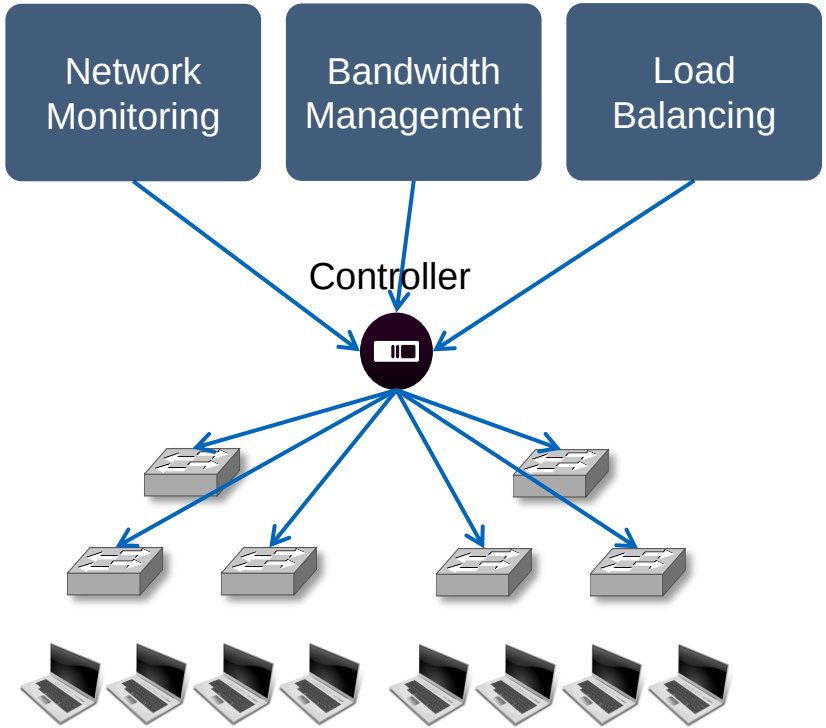
No policy resolution

Network Programmability

Programmatic Interface

onePK

OpenFlow

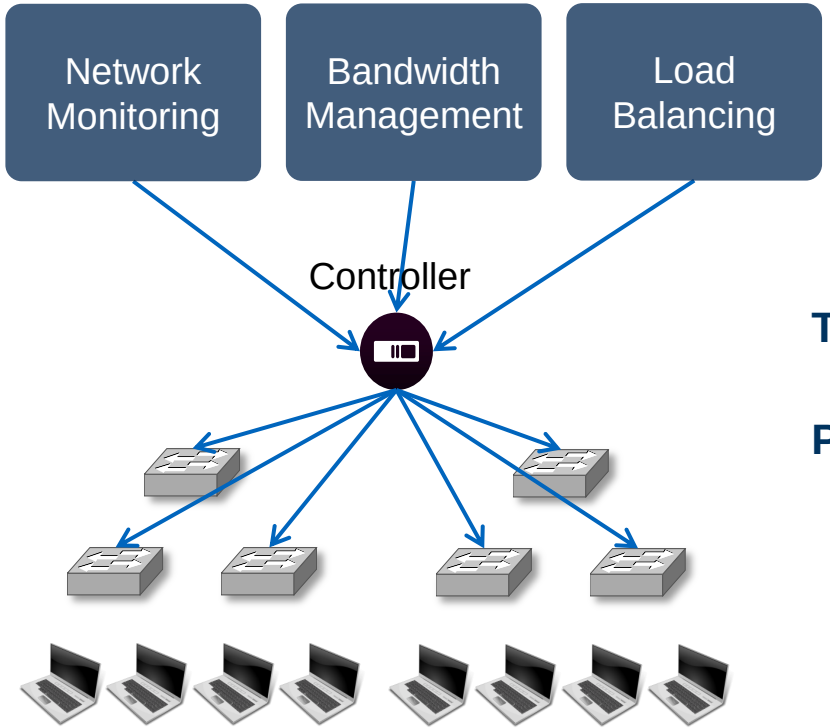


Network Programmability

Programmatic Interface

onePK

OpenFlow



Topological awareness

Policy resolution

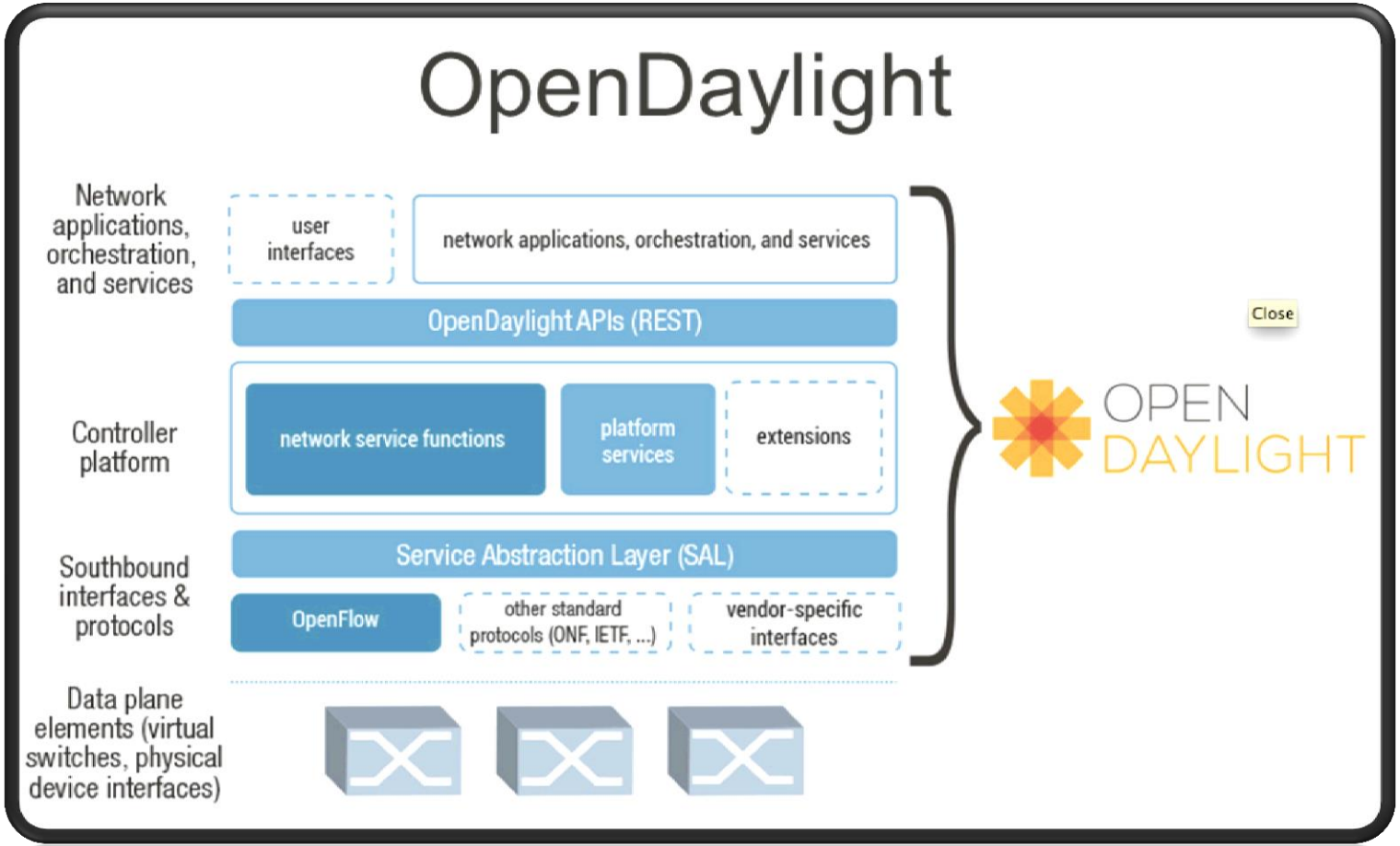
Cisco SDN

- Solves challenging next generation customer problems in Data Centre, Access and WAN
- Provide network wide abstraction
- Provide Business Agility so customer can roll out new applications and services quickly and cost effectively
- Automate infrastructure provisioning based on application policy profiles
- Secure multi-tenancy with centralised compliance and auditing
- Provide Open APIs for integration with existing systems and enabling a vast ecosystem of partners

Cisco Controllers

Open Day Light (ODL)

Open Source
OpenFlow
onePK



Credit: The Open DayLight Project, Inc.

Cisco Controllers

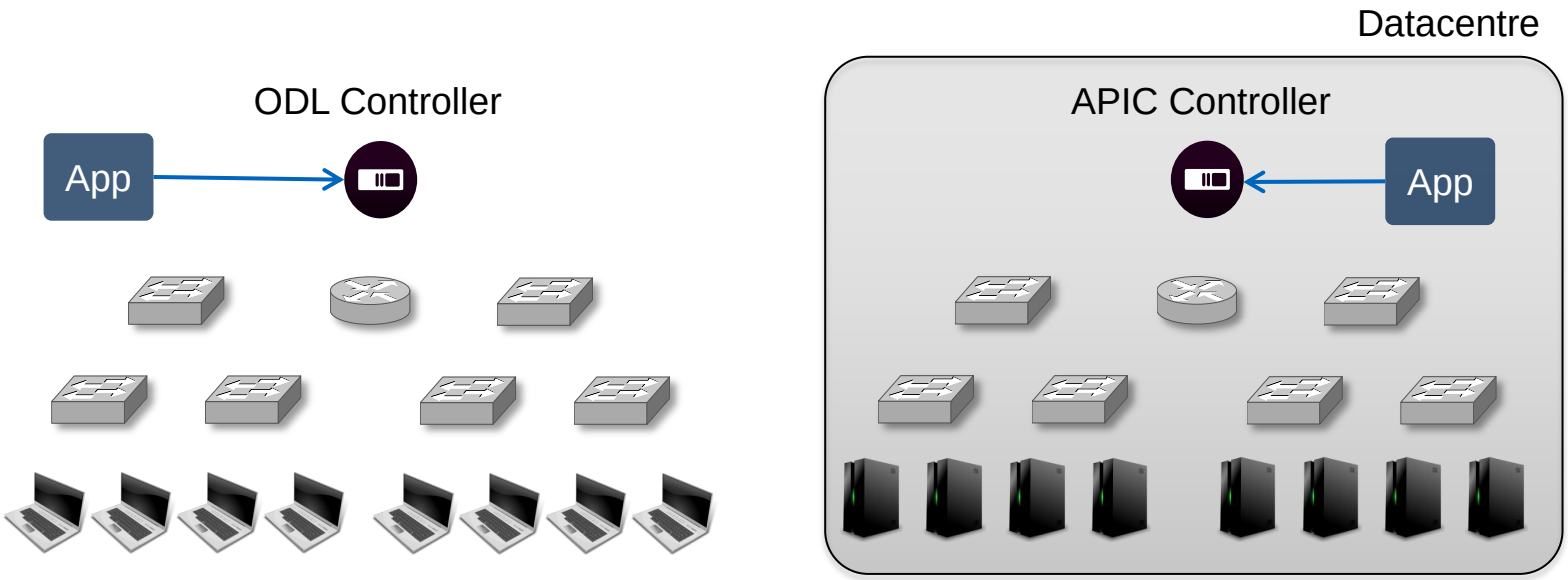
Open Day Light (ODL)

Open Source
OpenFlow
onePK

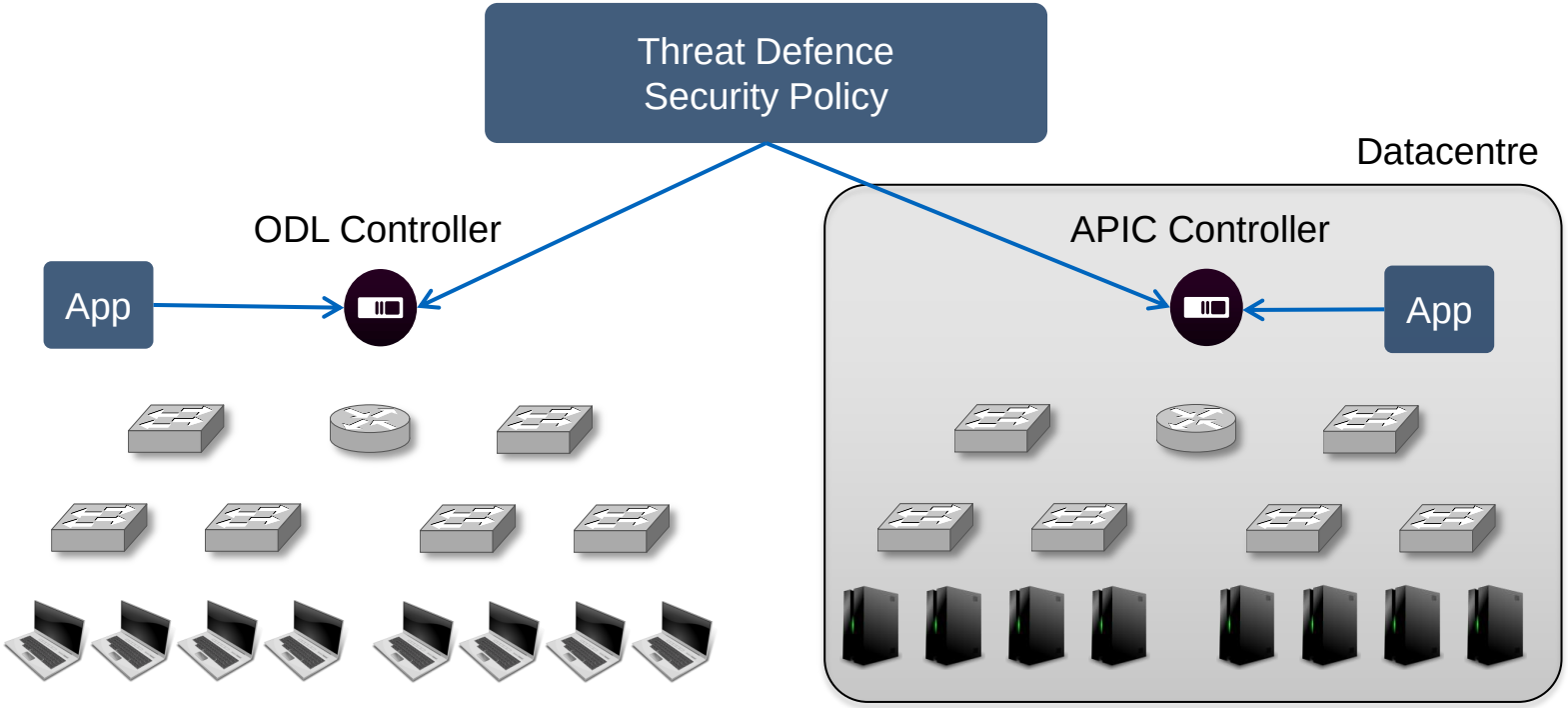
Application Policy Infrastructure Controller (APIC)

Application Centric Infrastructure Fabric
Physical, Virtual, and Cloud
Open APIs
OpenStack

Programmability Across Multiple Controllers

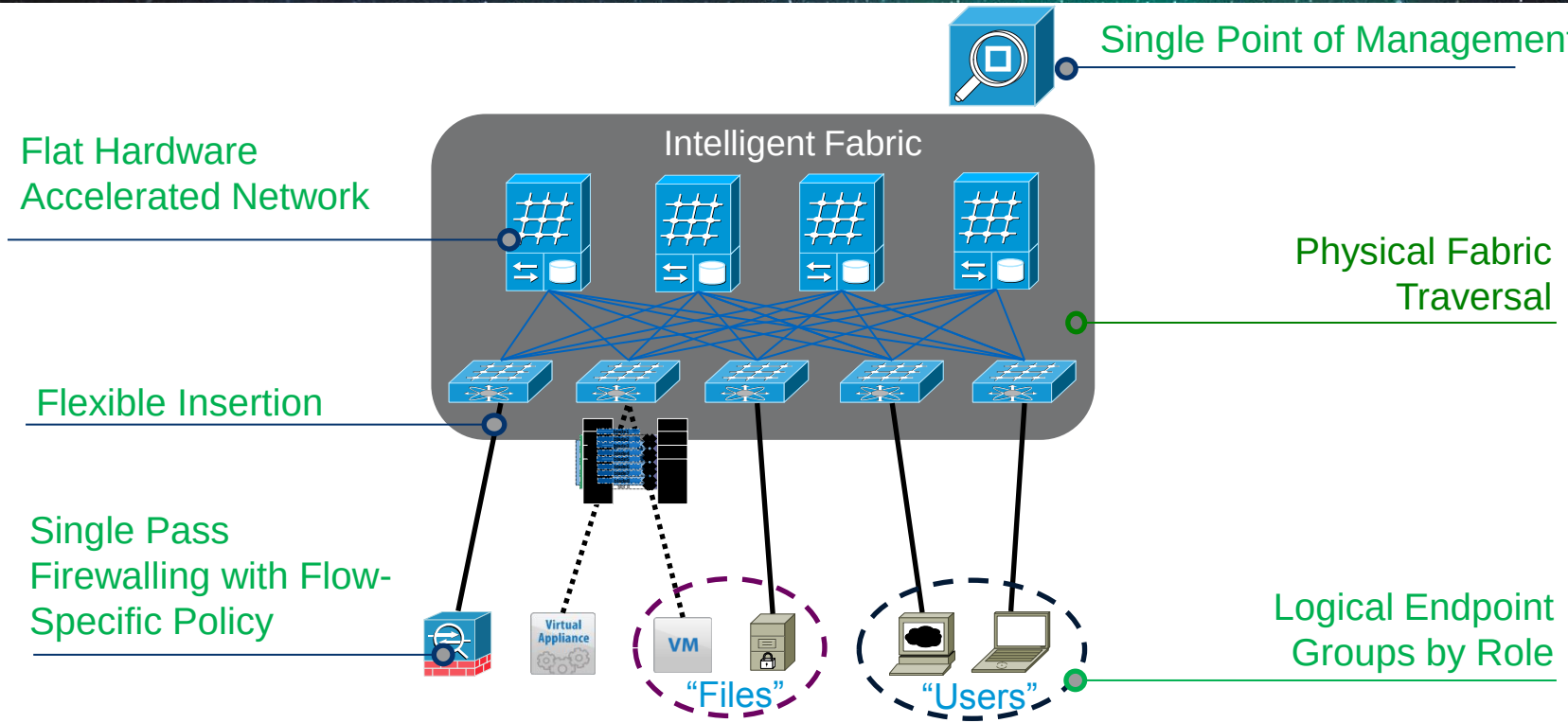


Programmability Across Multiple Controllers

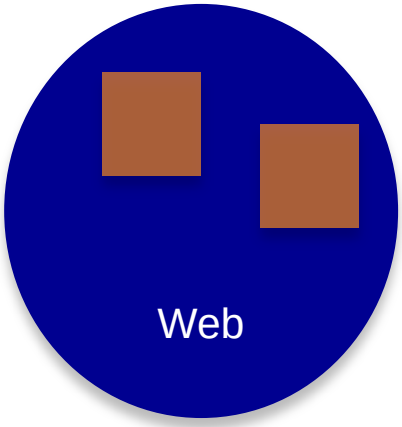


Application Centric Infrastructure

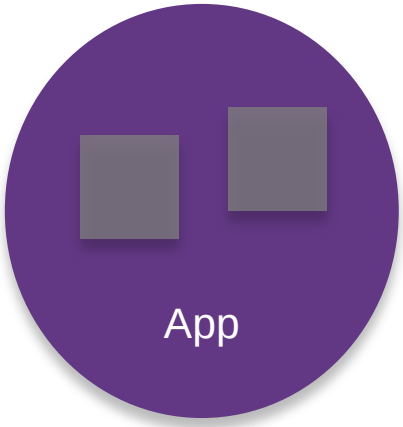
Application Centric Infrastructure Fabric



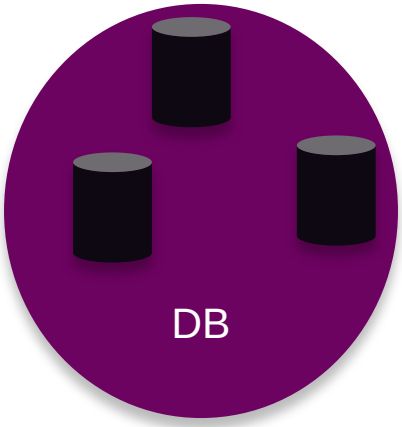
End Point Groups Simplify Policy



EPG 2

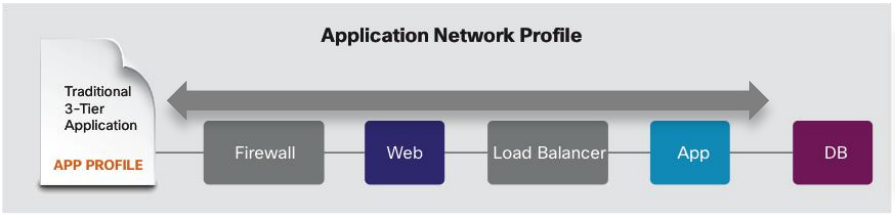


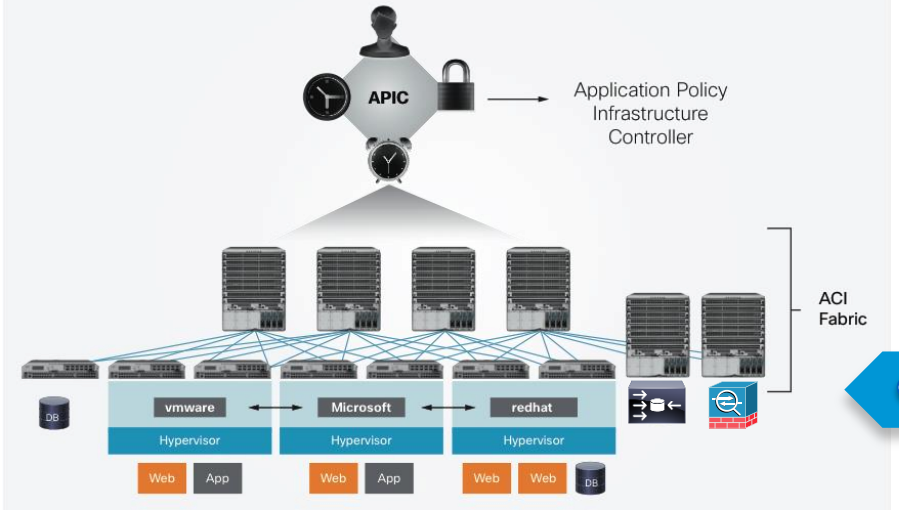
EPG 3

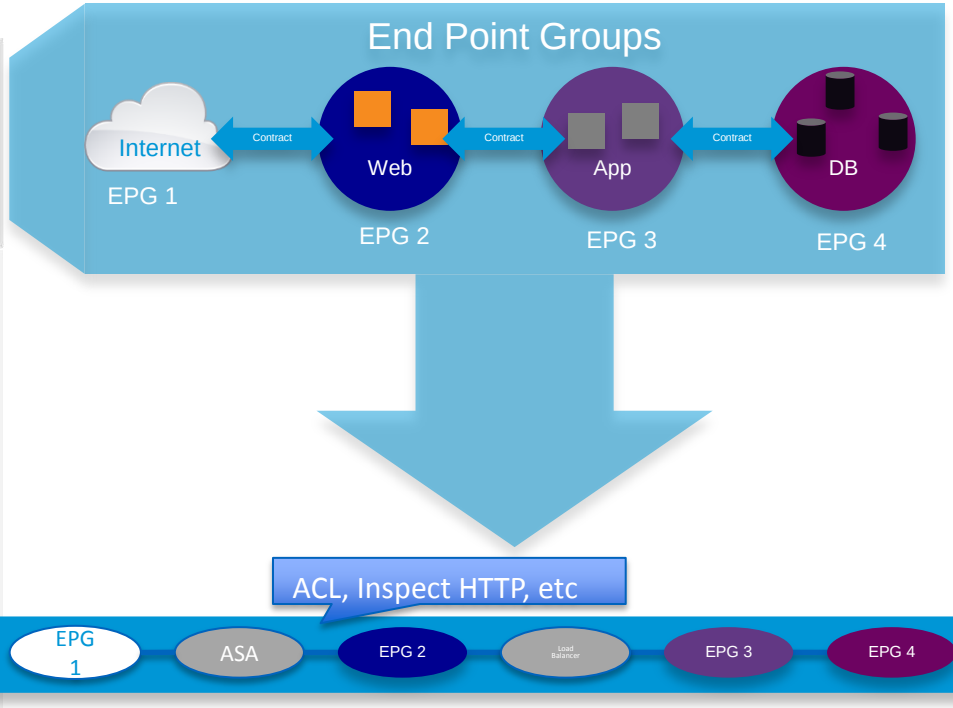


EPG 4

Service Insertion and ACI



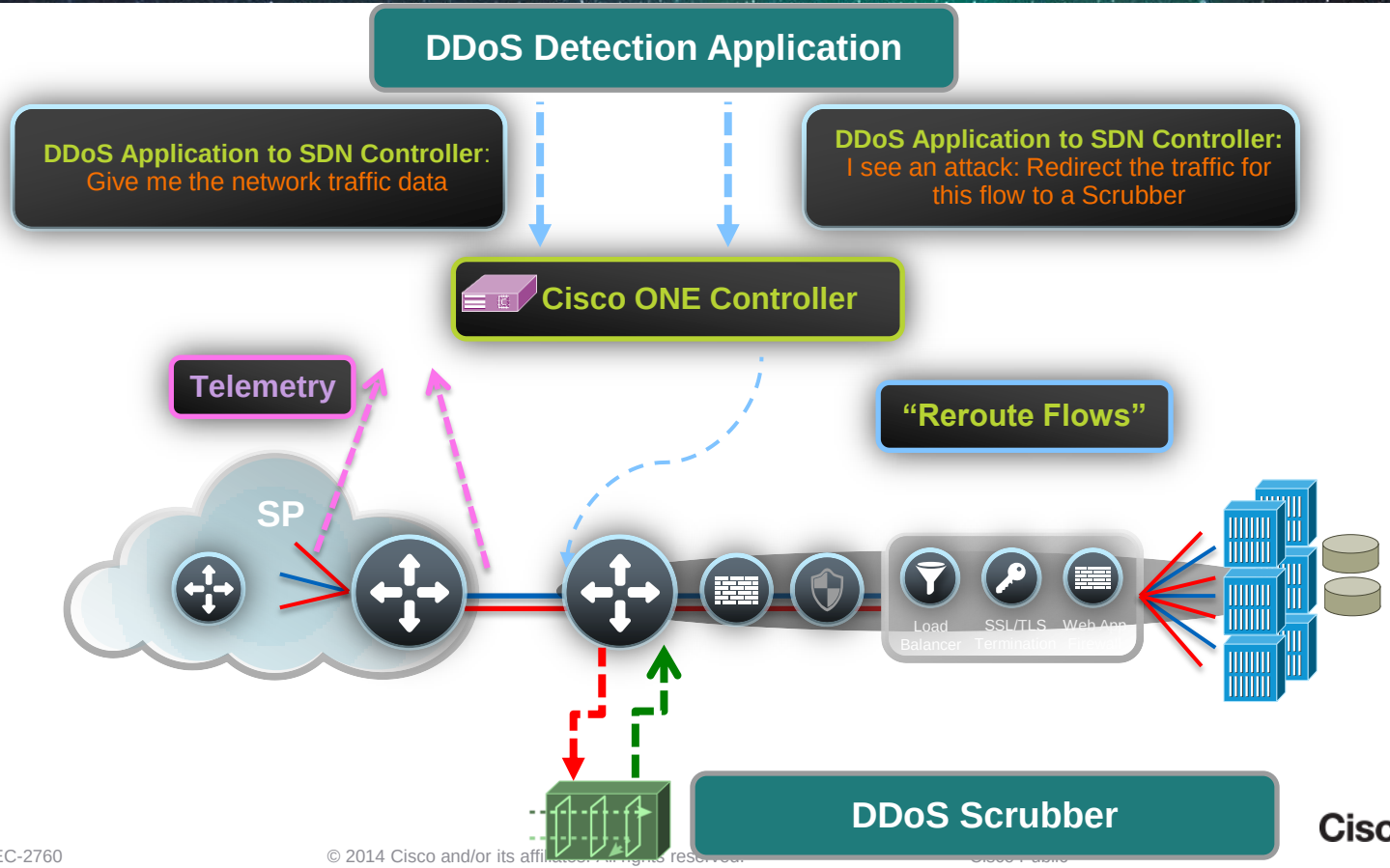






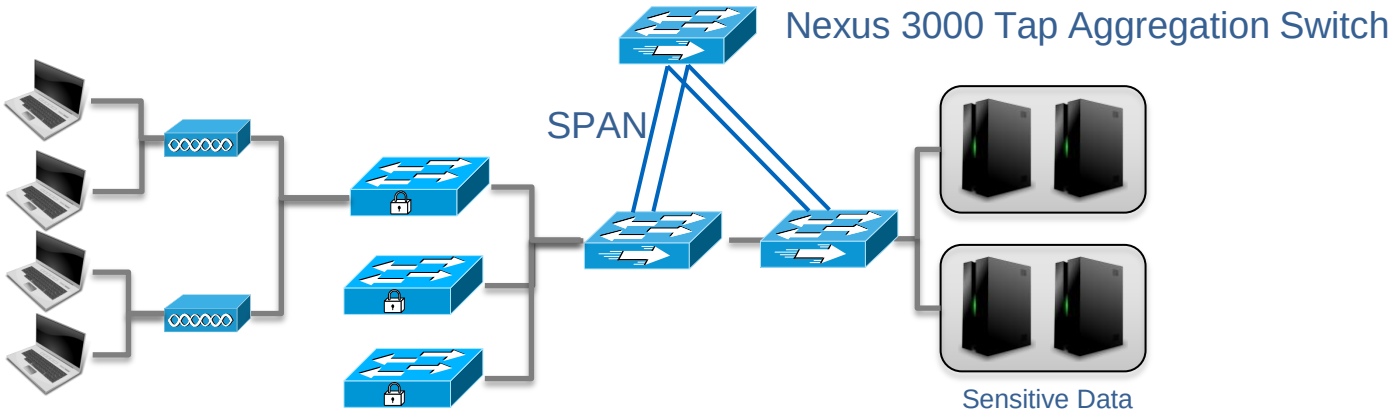

SDN and Security

Simple Example - DDoS Mitigation

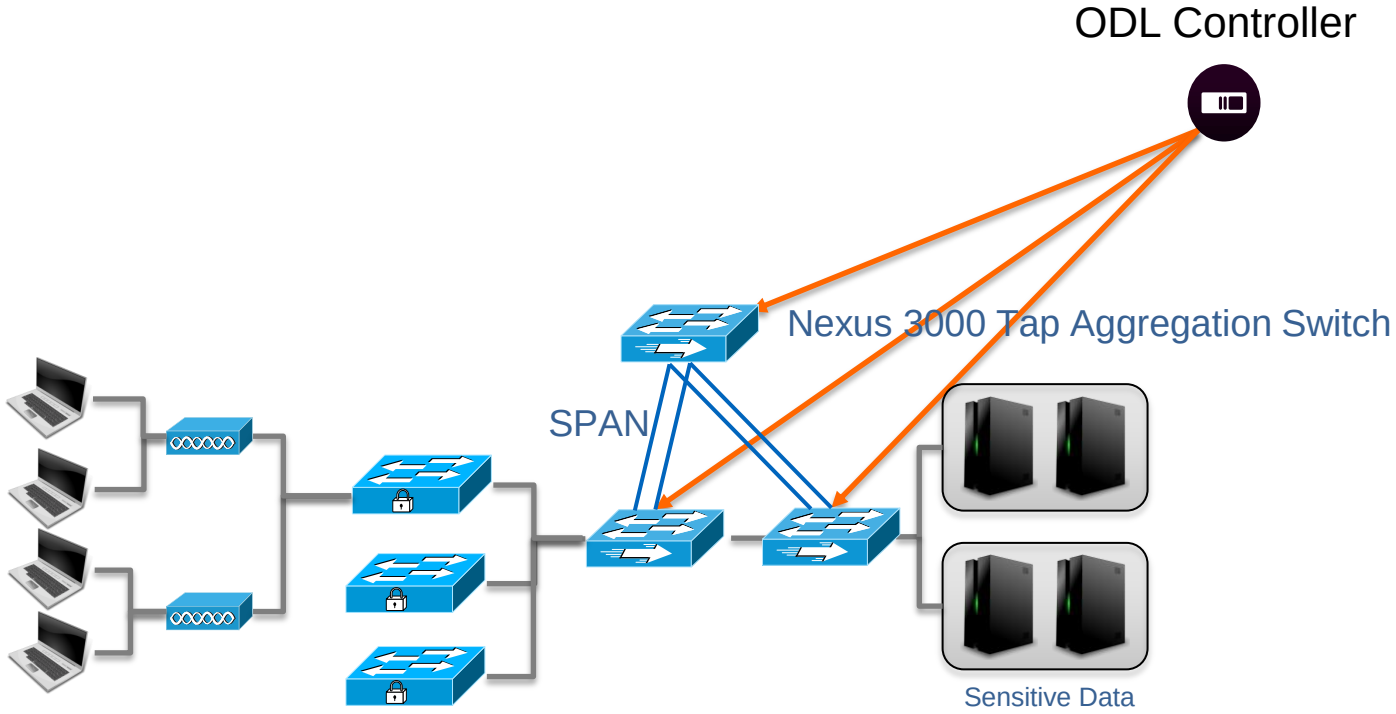


ODL Monitor Manager

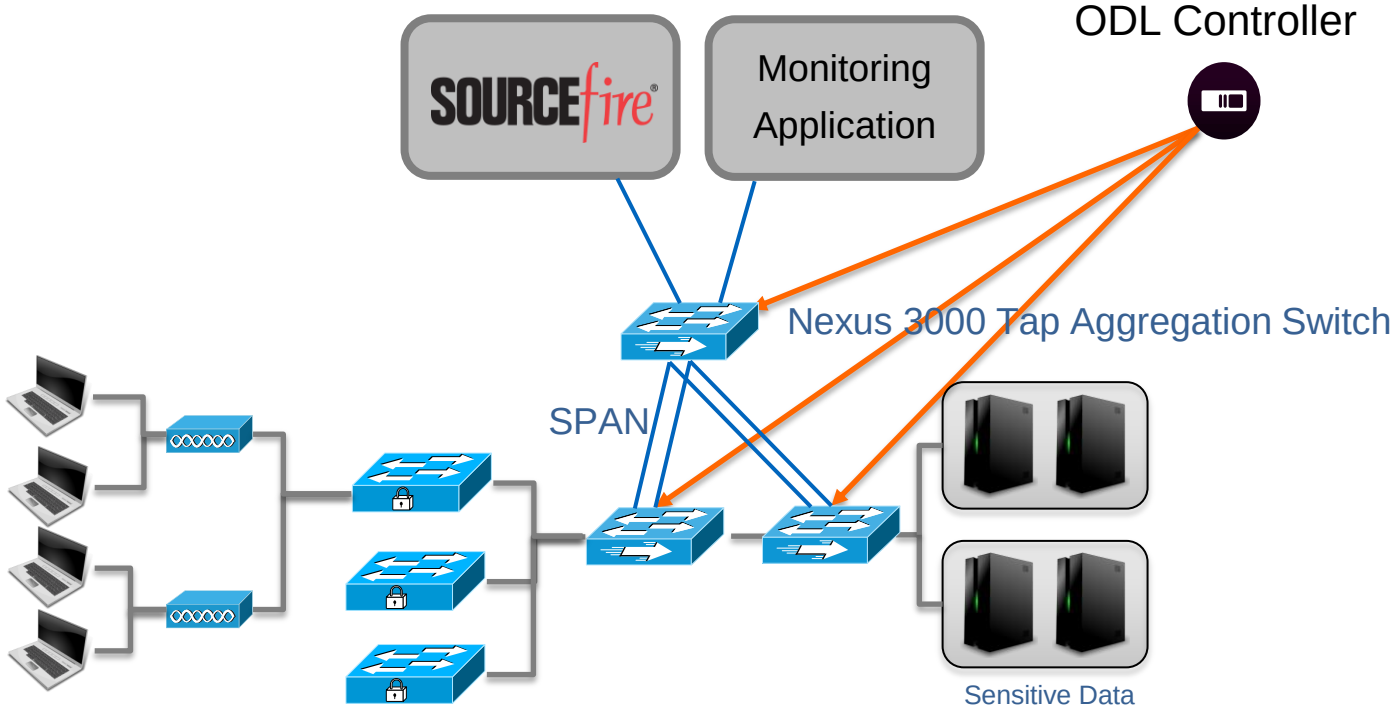
ODL Controller



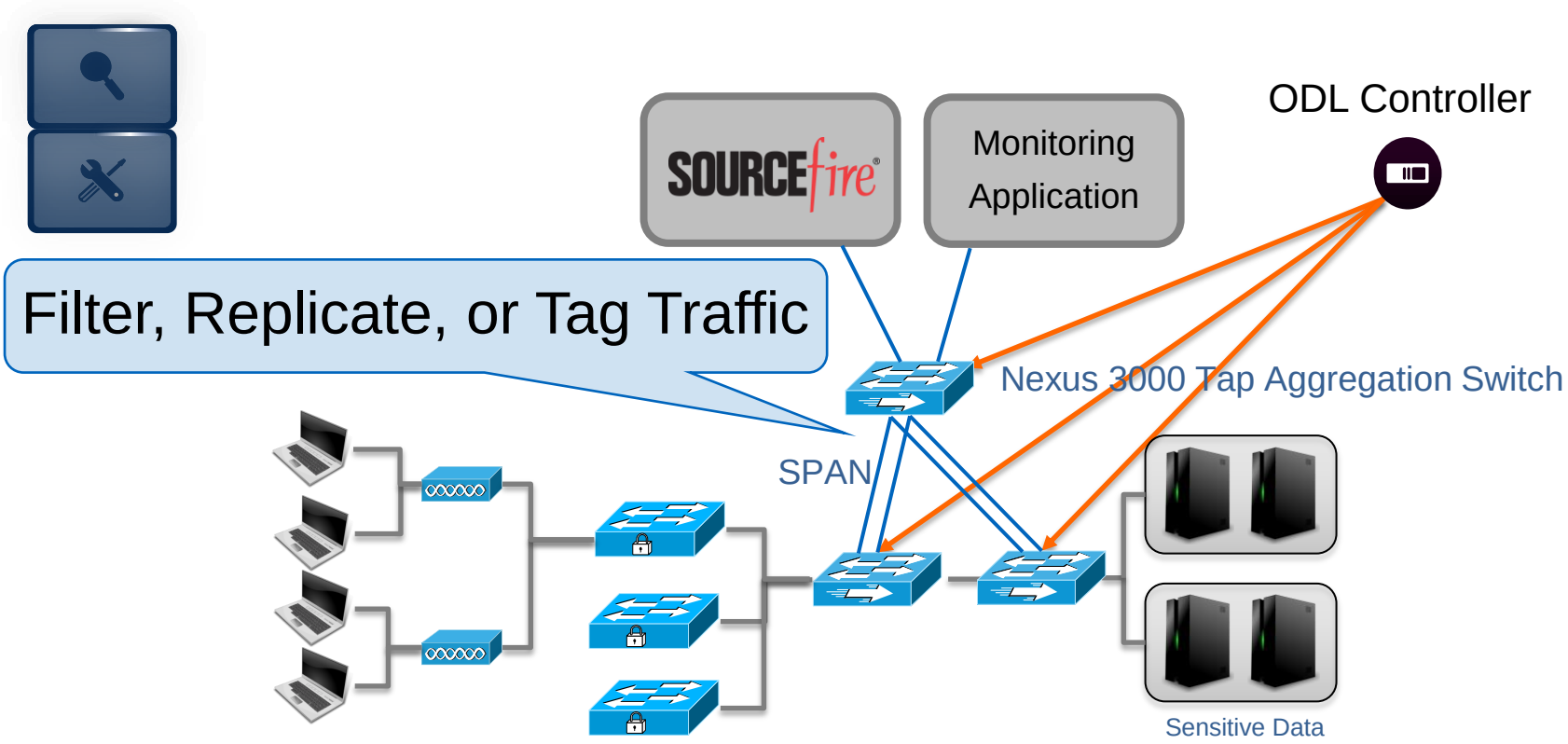
ODL Monitor Manager



ODL Monitor Manager



ODL Monitor Manager



What SDN Promises for Security

SIMPLIFY POLICY form a trusted path from user to application

CONVERGE INTELLIGENCE to more centralised security services

LEVERAGE THE NETWORK FOOTPRINT to redirect traffic, identify and block new and unknown threats

SIMPLIFY POLICY

Trusted Path from User to Application

Simplify Network Segmentation

- End-to-end VLANs
- Extend network segments over distance

Benefits

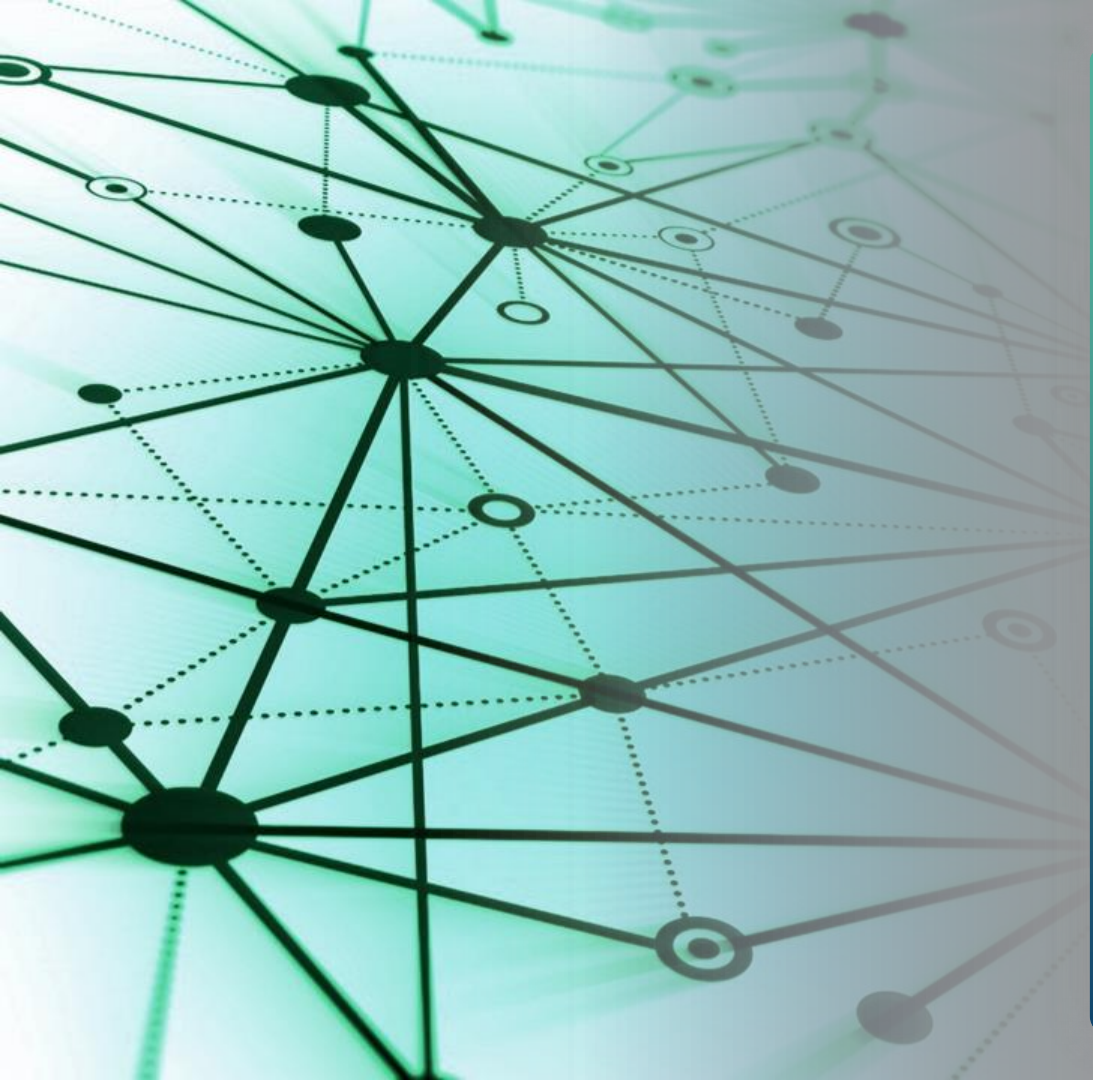
- Data confidentiality
- Multi-tenancy

CONVERGE INTELLIGENCE

Bring Network Flows to Central Security Services

Benefits

- Make the network far less complex



LEVERAGE THE NETWORK FOOTPRINT

Redirect Traffic for Analysis

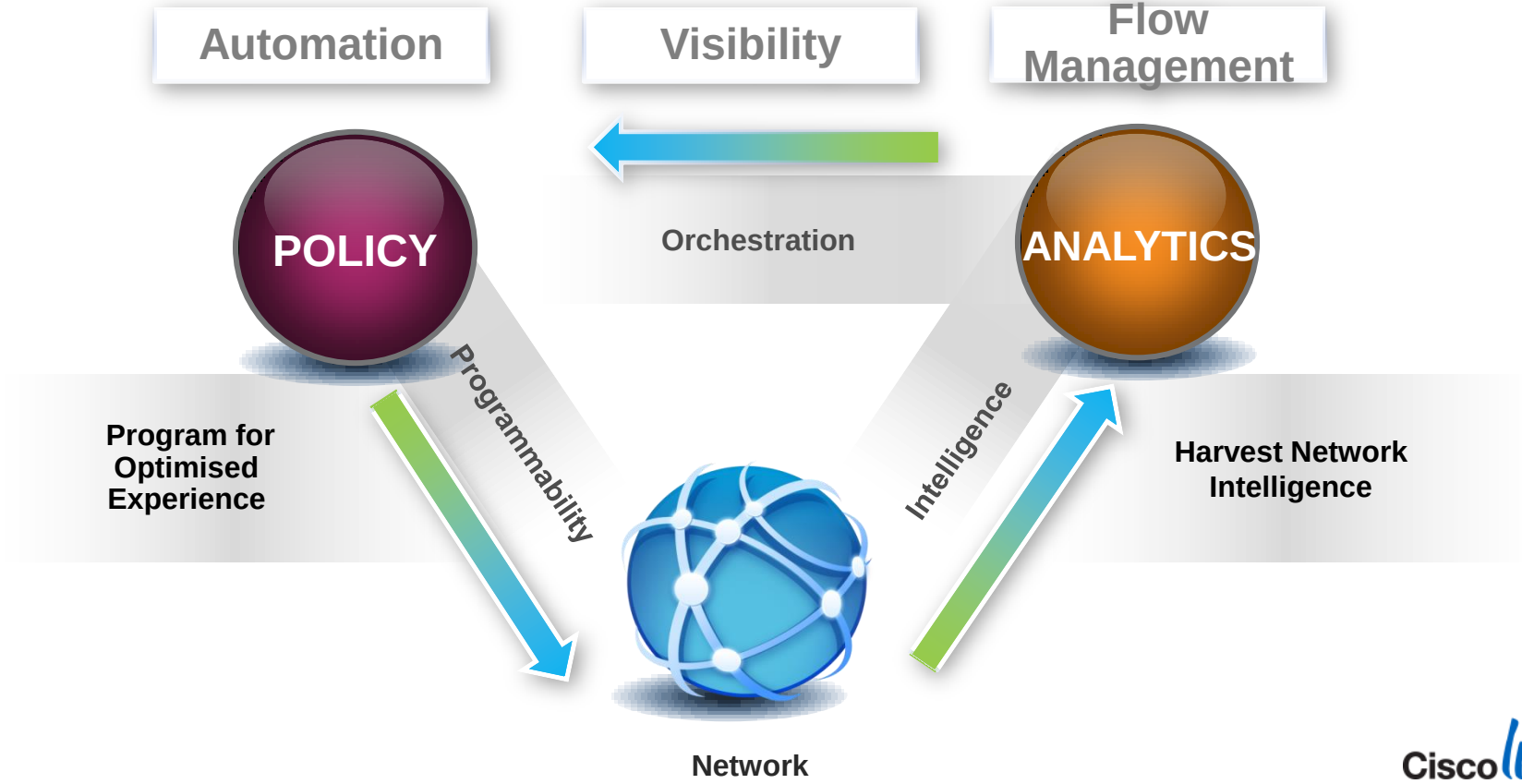
Automatically Identify Infected hosts for quarantine and remediation

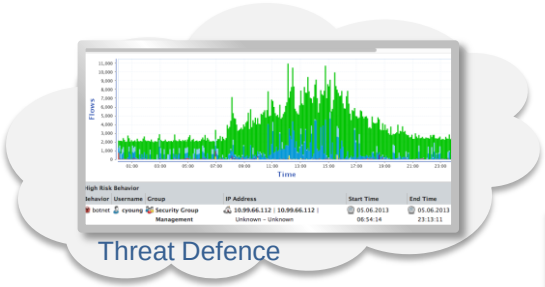
Dynamically provision network for threat protection

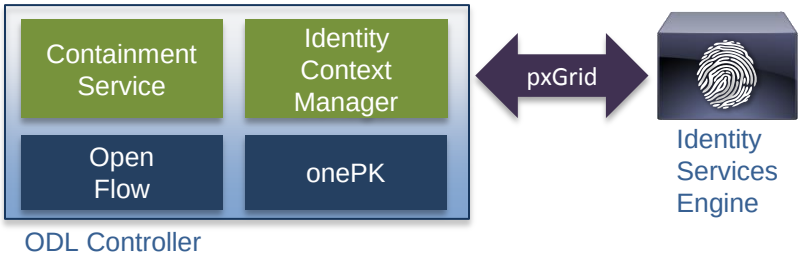
Benefits

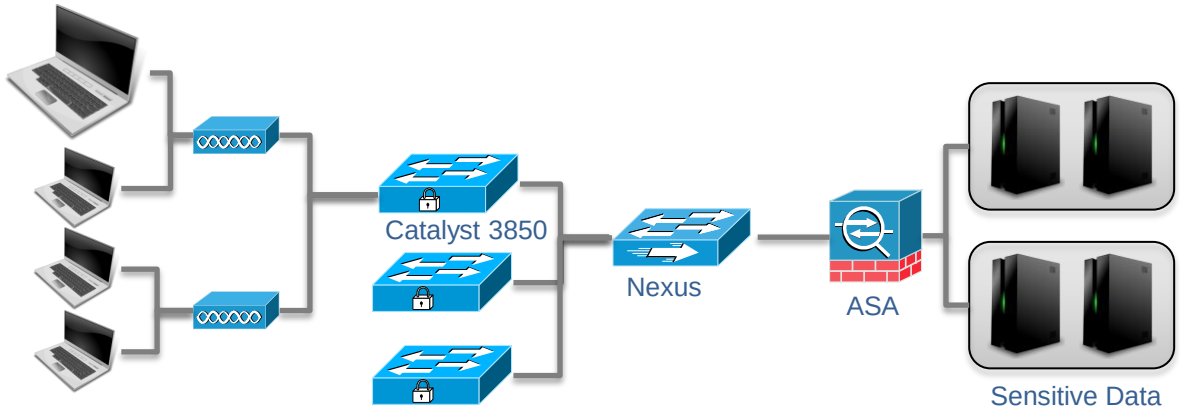
- Enhanced network visibility
- Dynamic threat response

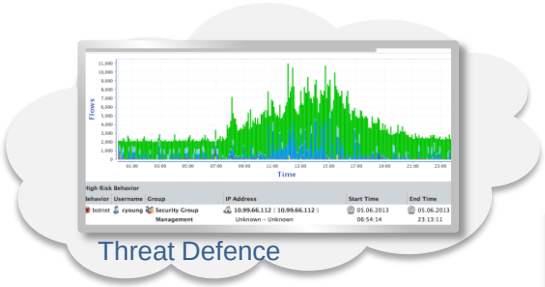
SDN Exposes Network Value

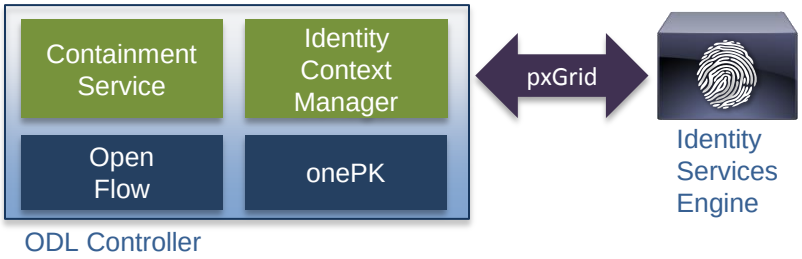


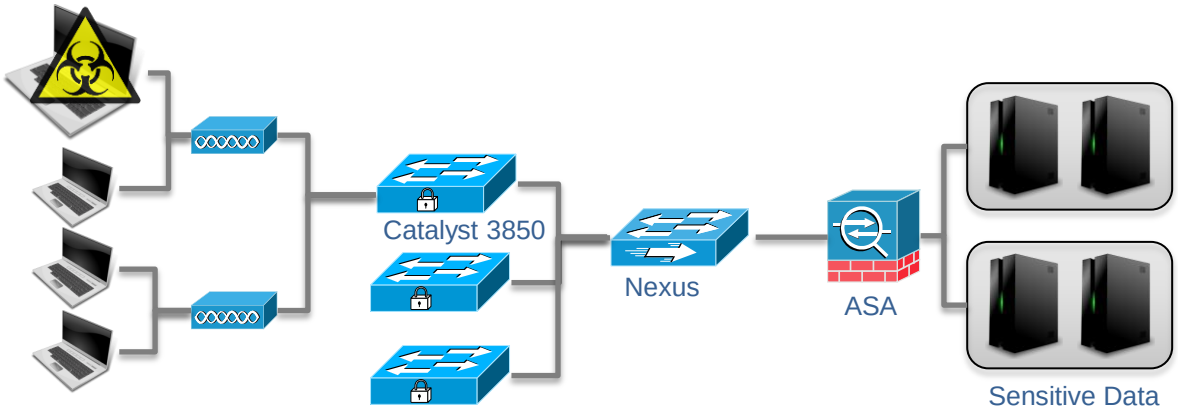


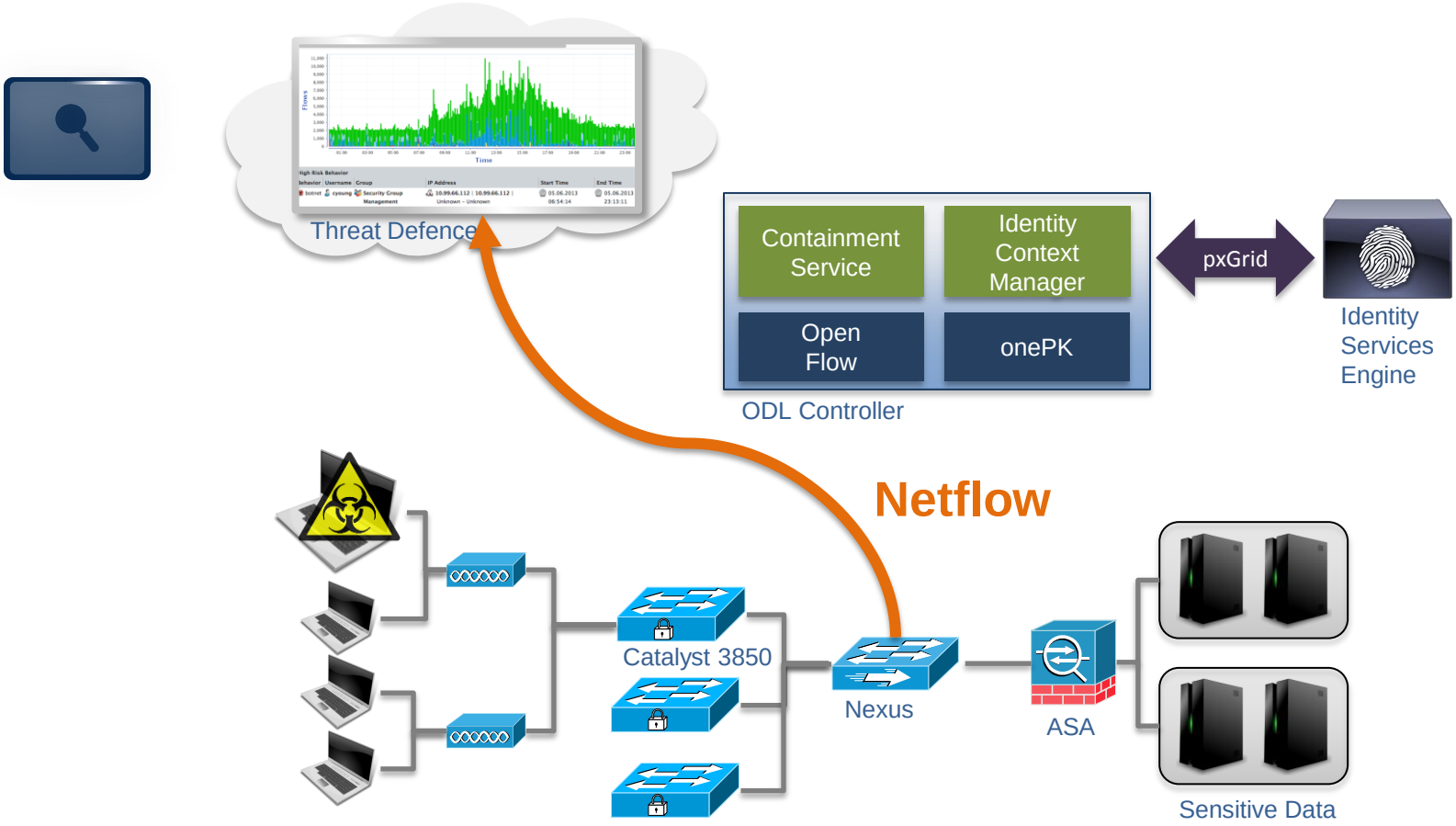


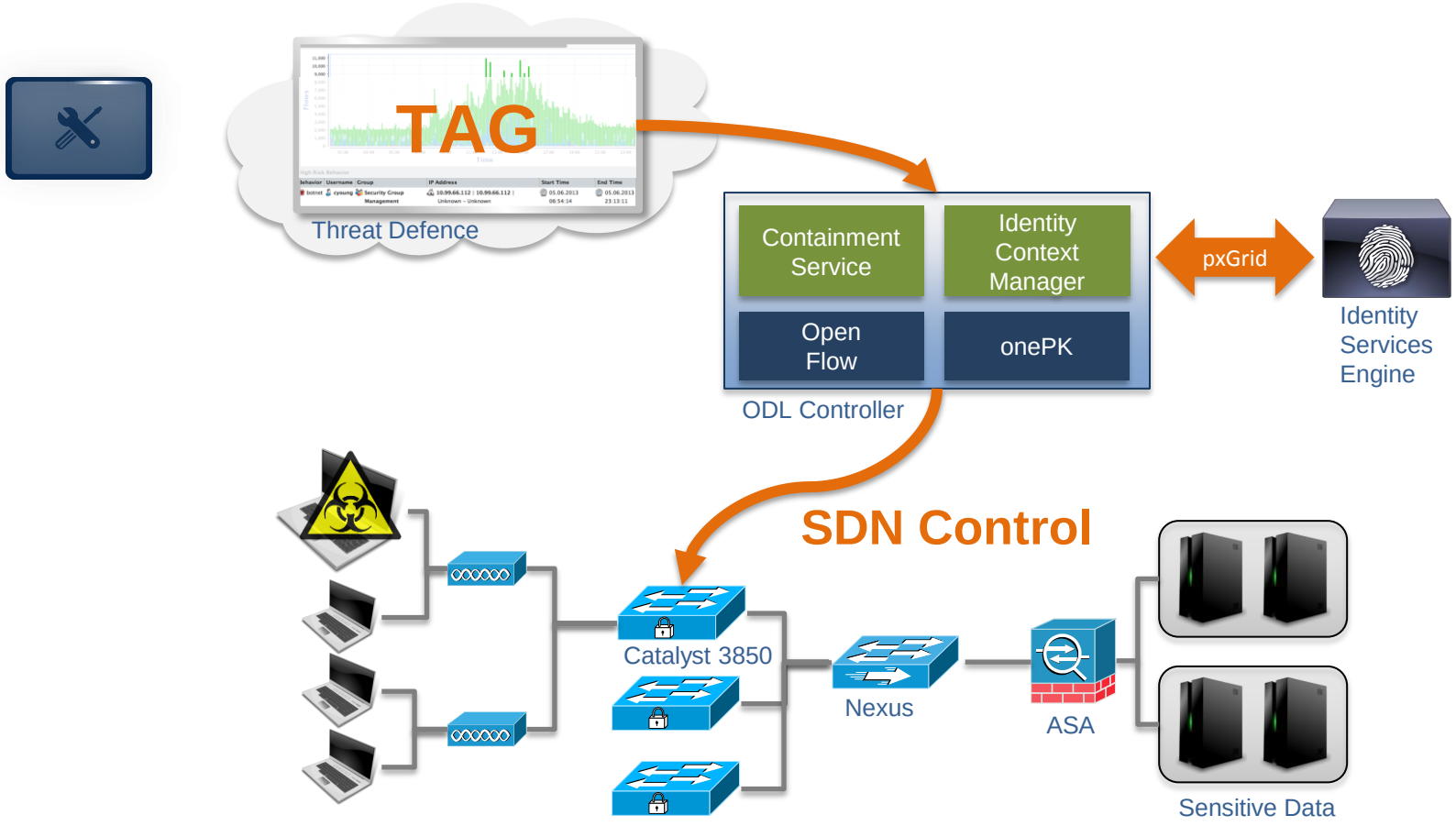


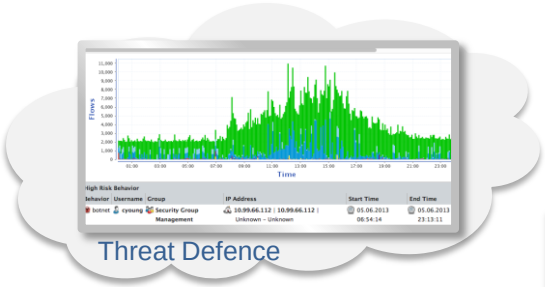


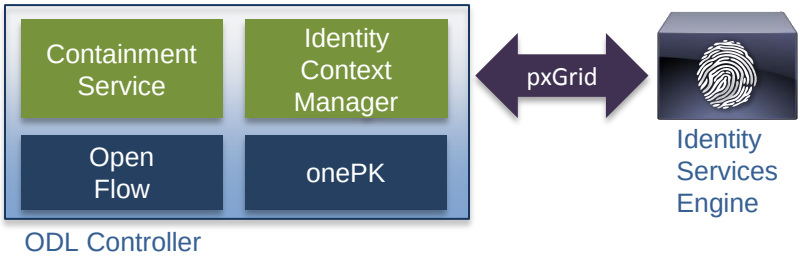




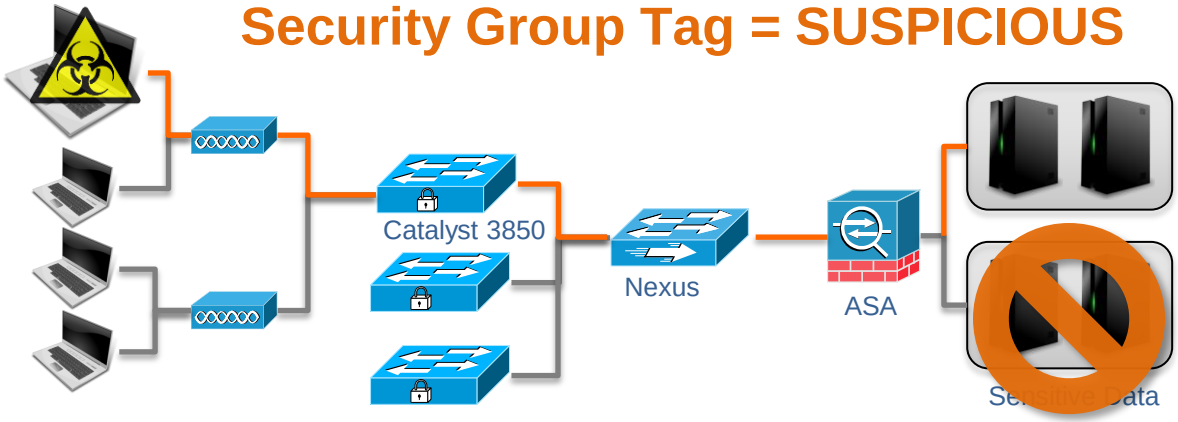


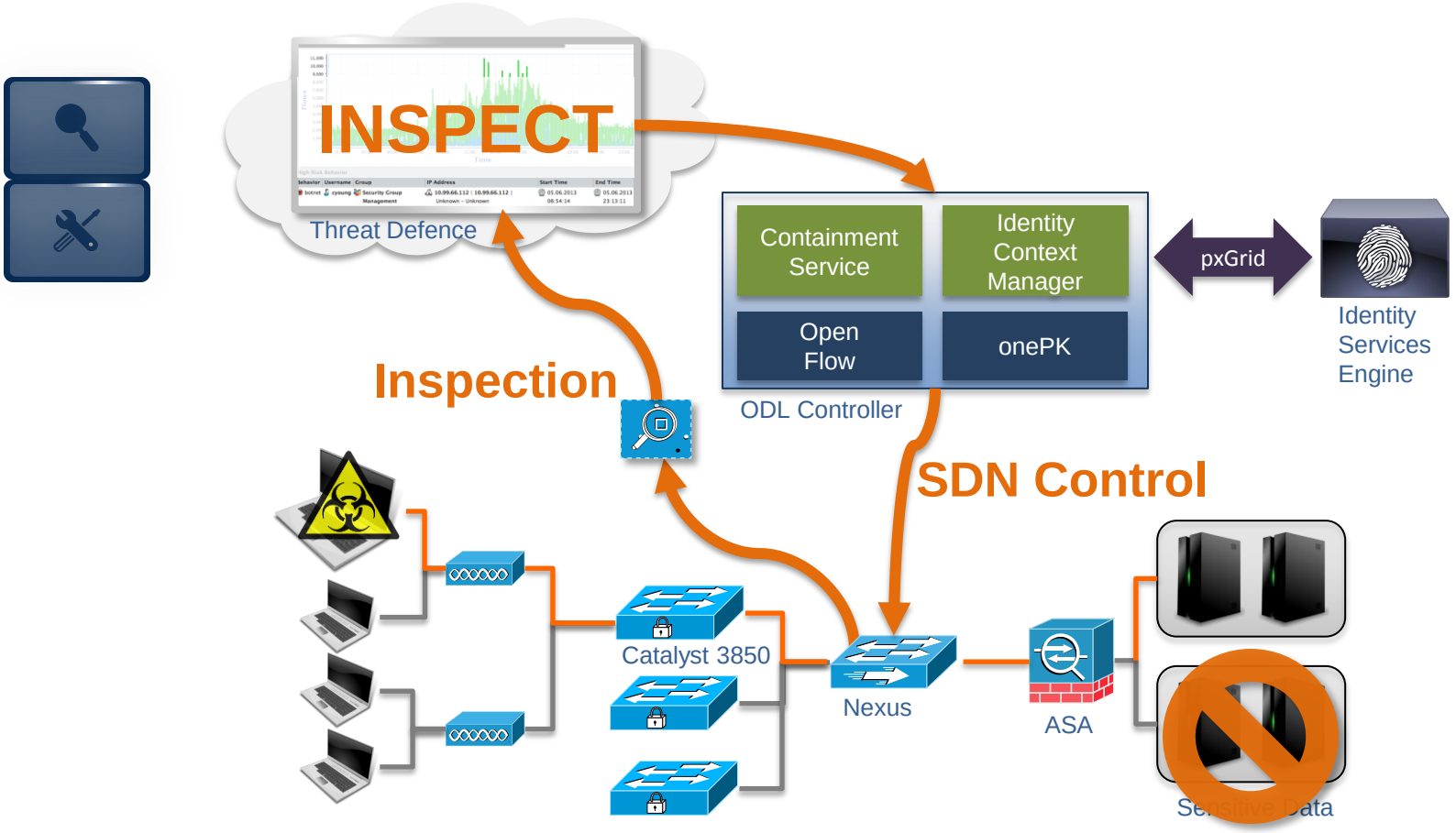


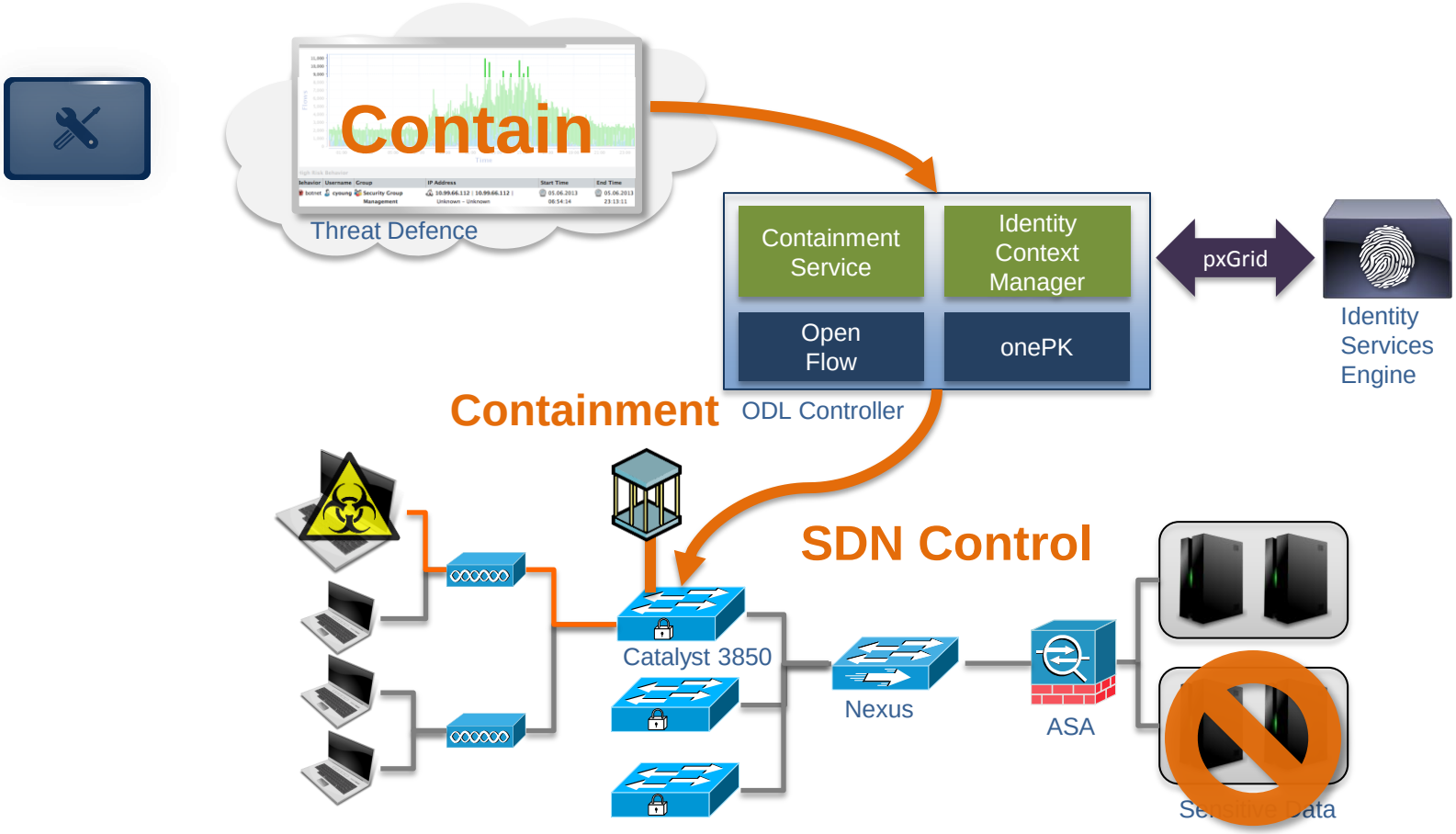


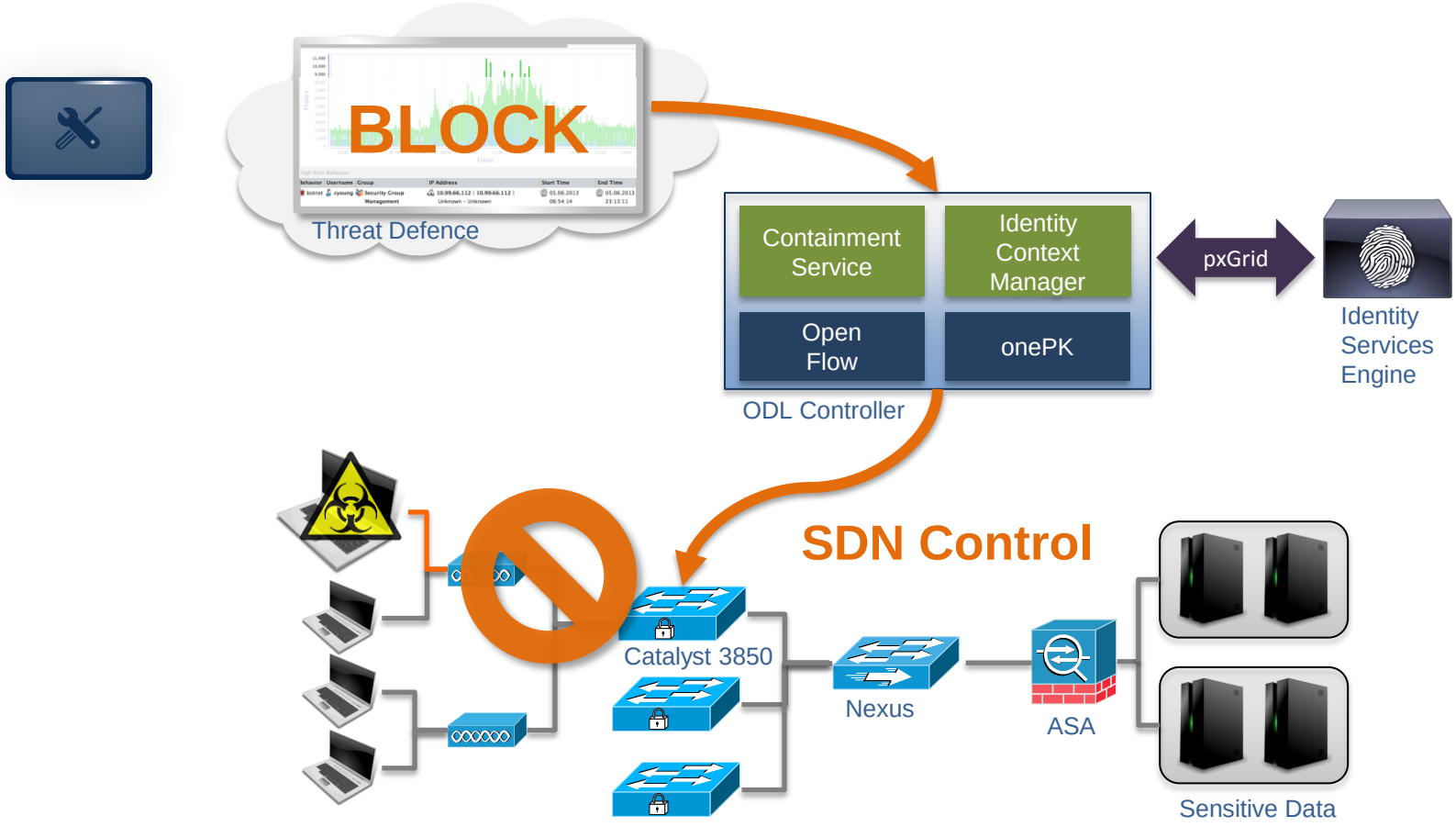


Security Group Tag = SUSPICIOUS



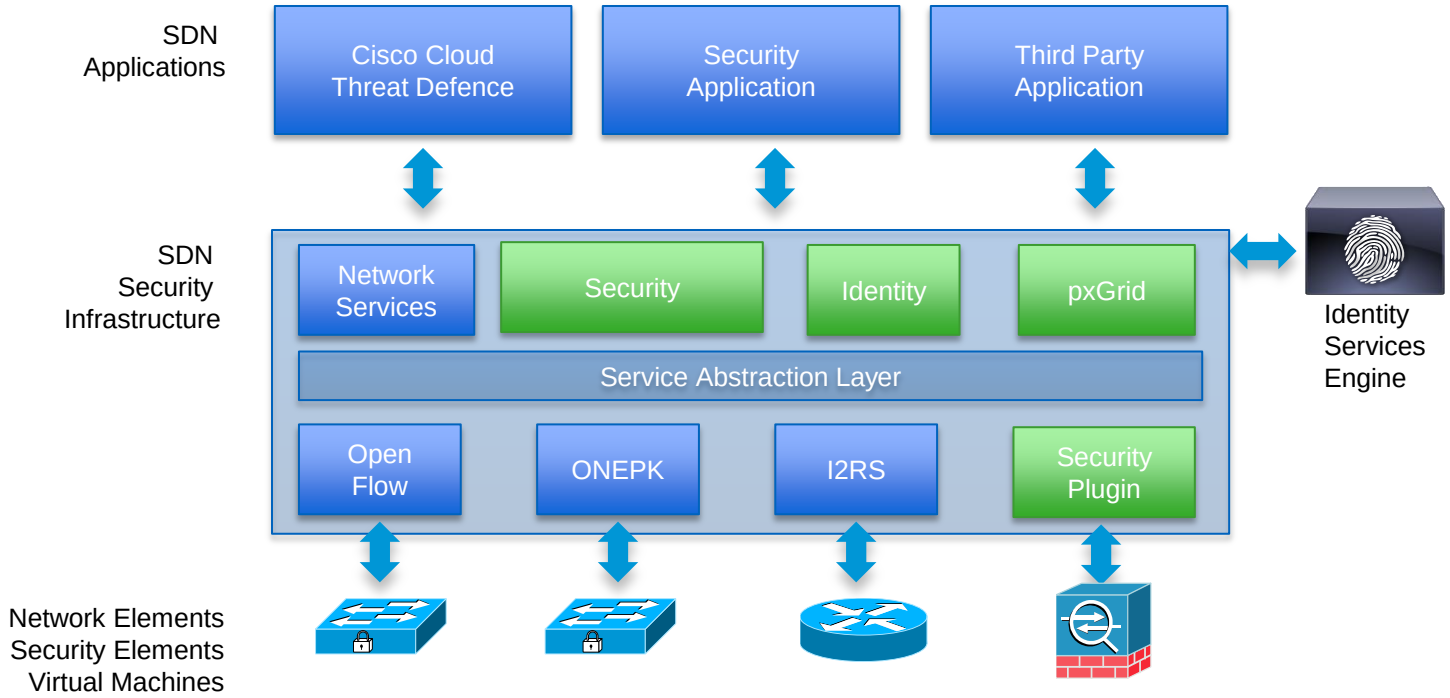




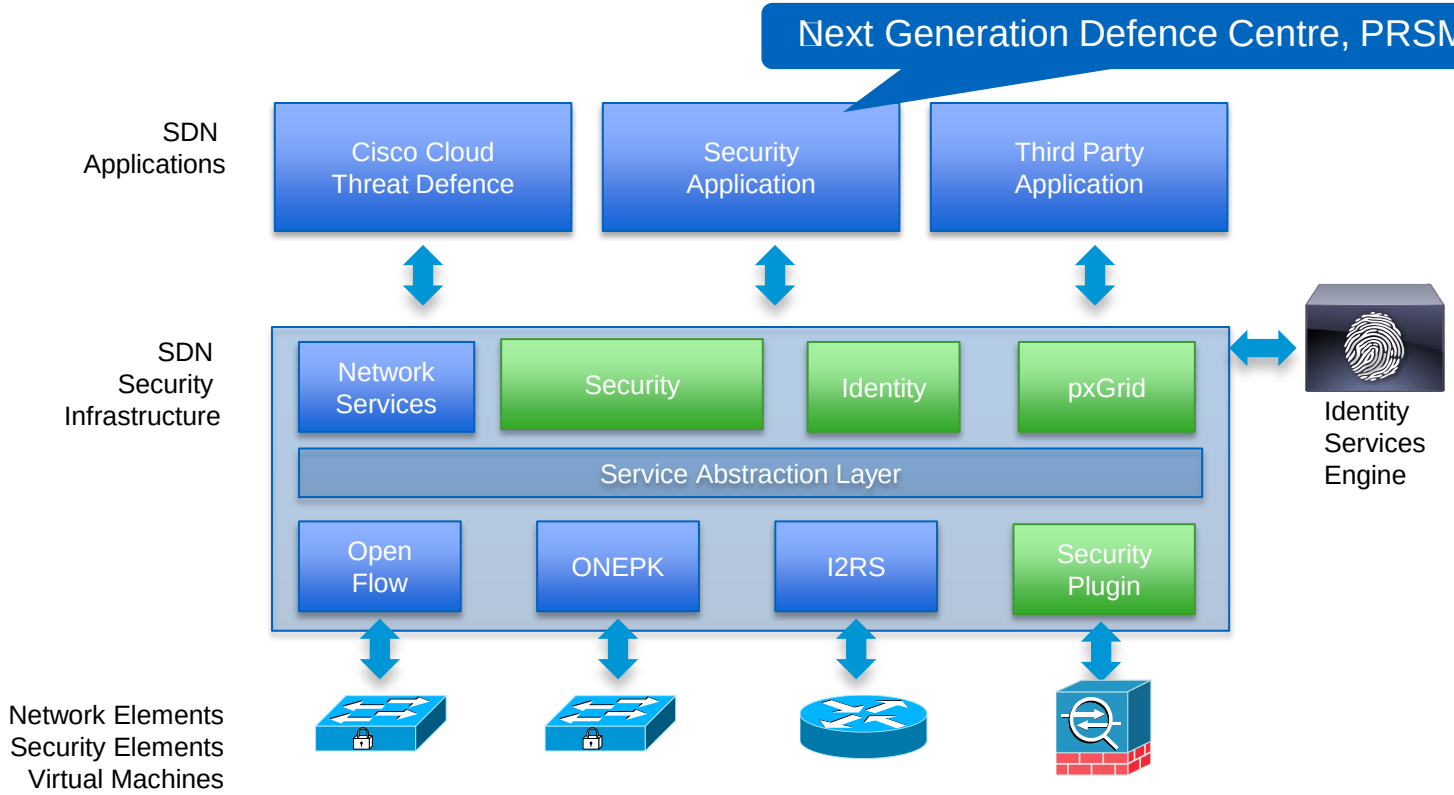


SDN Security Components

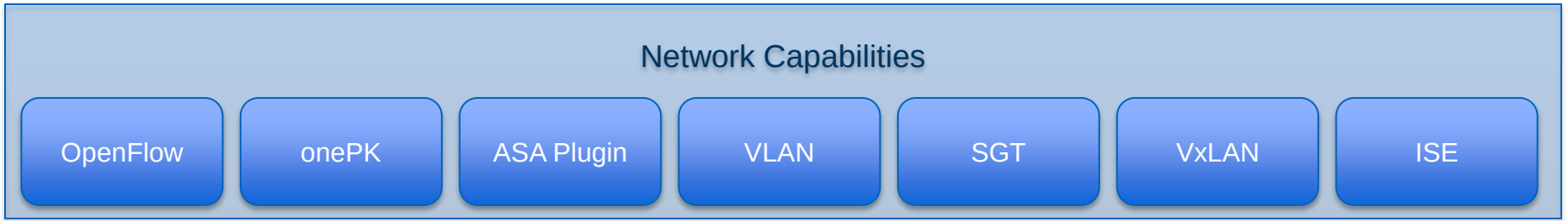
SDN Security Components



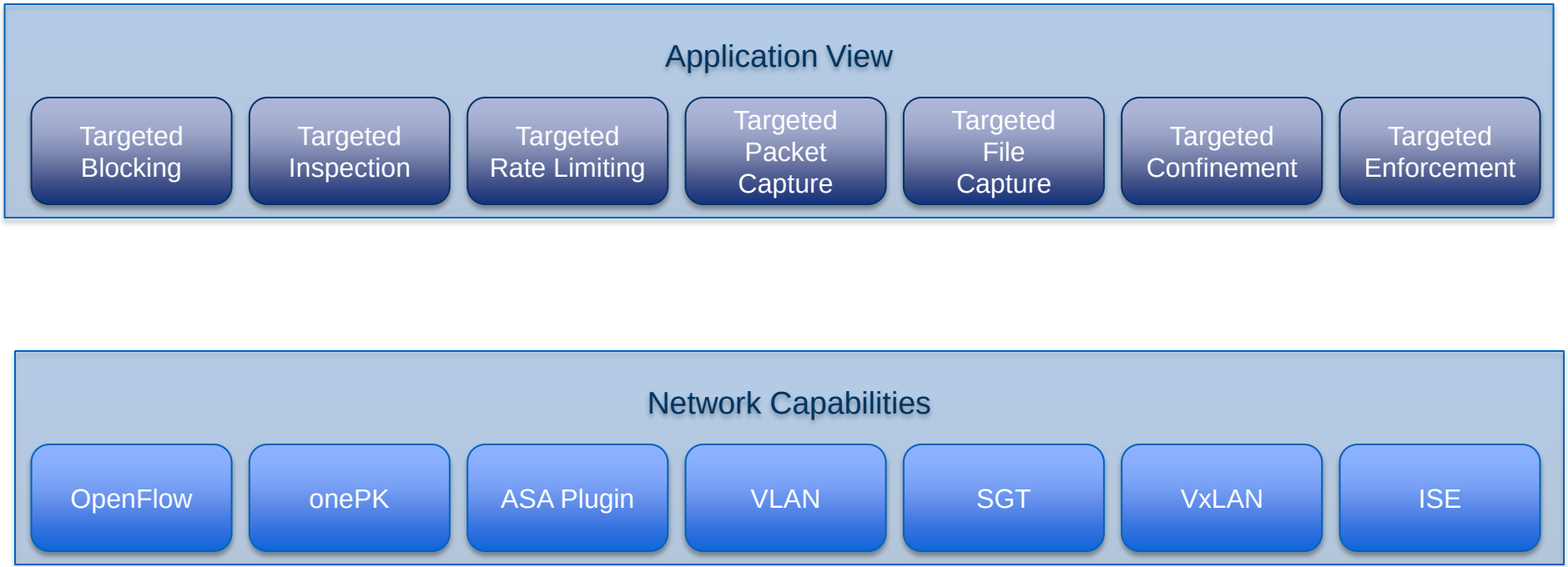
SDN Security Components



Threat Defence Services



Threat Defence Services



Security Services Through SDN

Audit

Recording

Monitoring

Inspection

Rate Limiting

DDoS Scrubbing

Quarantine

Active Web Firewall

Blocking

Security Services Through SDN

Audit

Recording

Monitoring

Inspection

Rate Limiting

DDoS Scrubbing

Quarantine

Active Web Firewall

Blocking

Security Services Through SDN

Audit

Recording

Monitoring

Inspection

Rate Limiting

DDoS Scrubbing

Quarantine

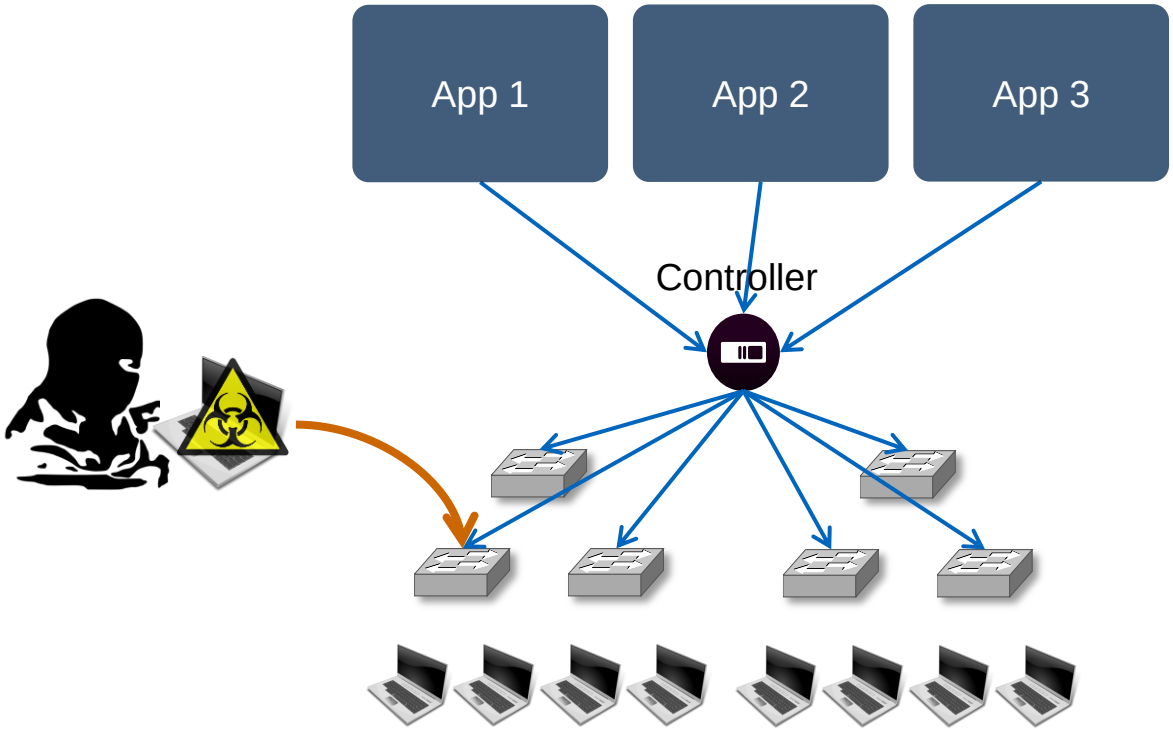
Active Web Firewall

Blocking

Network Controller Reconciles Mitigations Against the Needs of Mission-critical Applications

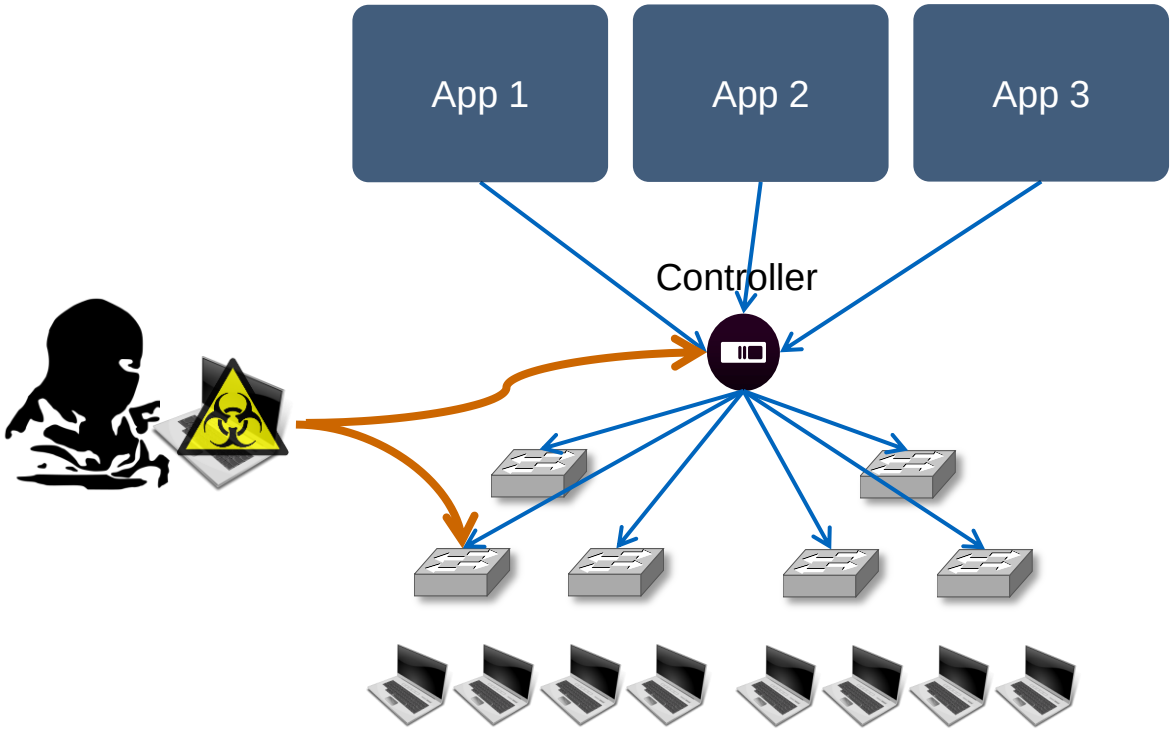
Securing SDN

Threats to an SDN System



Spoofing Controller to Network Element Communication

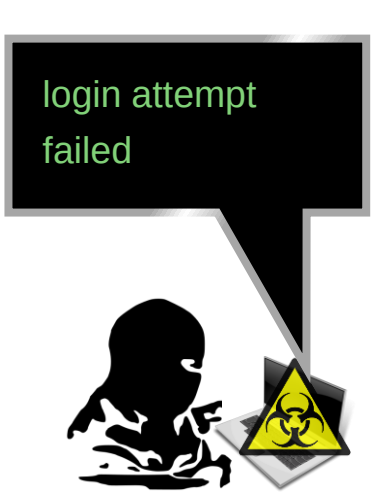
Threats to an SDN System

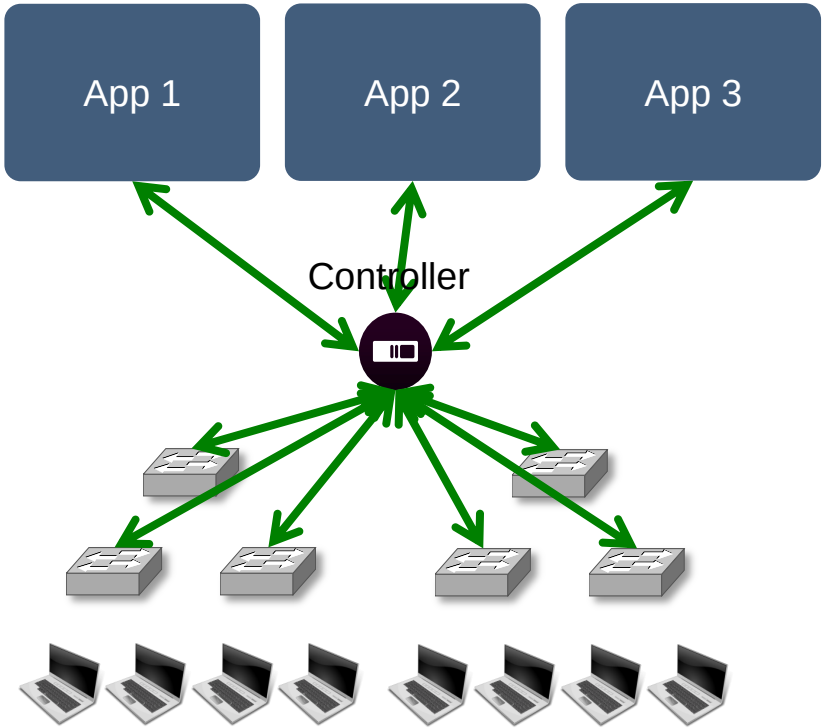


Spoofing App to Controller Communication

Spoofing Controller to Network Element Communication

Securing SDN





Authentication
Authorisation




Considerations

Considerations

Detection

- How automated is your telemetry capture?
- How automated is your threat analysis?
- Are you limited by privacy considerations?

Considerations

Detection

- How automated is your telemetry capture?
- How automated is your threat analysis?
- Are you limited by privacy considerations?

Response

- What actions are you willing to take in real time?
- What actions should be one-click for a security analyst?

Considerations

Detection

- How automated is your telemetry capture?
- How automated is your threat analysis?
- Are you limited by privacy considerations?

Response

- What actions are you willing to take in real time?
- What actions should be one-click for a security analyst?

SDN

- What type of SDN can you use?
- How SDN-ready is your network?
- SDN security?




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com


CISCO
TM